AMENDMENT No. 1 TO:
Orange County Master Agreement
MA-017-19010780
Between
Microsoft Corporation and County of Orange - OCIT

THIS AMENDMENT No. 1 TO Master Agreement MA-017-19010780 (the "Amendment") is made and entered into effective as of the Effective Date identified below by and between the undersigned for the purpose of amending that certain Master Agreement MA-017-19010780 (the "Agreement"), by and between County of Orange – OCIT ("Customer" or "you") and Microsoft Corporation.

Capitalized terms used herein and not otherwise defined have the meanings set forth in the Agreement.

In consideration of the promises, and for other good and valuable consideration, the receipt and sufficiency of which are acknowledged, the parties agree as follows:

1. Attachment B to the Agreement (Scope of Work) is hereby deleted in its entirety and replaced by the new Attachment B, which follows below.

2. Attachment C to the Agreement (Compensation and Payment) is hereby deleted in its entirety and replaced by the new Attachment C, which follows below.

3. All other terms and conditions shall remain unchanged. The Agreement shall remain in full force and effect as modified by this Amendment.

IN WITNESS WHEREOF, the parties have signed this Amendment on the date indicated below. This Amendment is not binding until executed by Microsoft.

MICROSOFT CORPORATION

By: DocuSigned by: David J. Gallagher C5F4FFFE6A2E45D

David T. Gallagher

Director of Contracts

11/22/2019

Effective Date

COUNTY OF ORANGE - OCIT

By: Joel Golub

JOEL GOLUB

Name

CIO

Title

11/22/2019

Date

ATTACHMENT B
SCOPE OF WORK

1 Project Objectives and Scope

1.1 Objectives

The purpose of this project is to design and implement an identity and access management solution for Orange County based on Microsoft Identity Manager (MIM) 2016. This solution will facilitate the management of user, contact and group objects in 27 Active Directory (AD) domains contained in 18 AD forests as well as the OCProfile SQL database from the MIM Portal. It will also help automate the management of user accounts and associated entitlements based on the data imported from the HR system.

This project will also perform a synchronization of mail contacts between 18 Microsoft Exchange organizations which are associated with the 18 in-scope AD forests.

1.2 Areas Within Scope

1.2.1 General Project Scope

Microsoft will provide services in support of the following scope.

Table 1: Services in Scope

Service, Feature or Function	Description	Key Scope Assumptions
Conduct Envisioning and Assessment workshops	• Assess the current environment to understand how identities are managed today • Collect customer requirements • Assess the 27 in-scope Active Directory domains and their synchronization of identity data to the OC-Global domain and the OCProfile database.	Customer stakeholders and subject matter experts (SMEs) will participate in workshops
Global Address List Synchronization	• Assess the current Orange County messaging environment to understand which portions of that environment will be in scope.	GAL Synchronization will only include the 18 in-scope AD forests and MS Exchange organizations
Access controls	Design and implement access controls for each persona who will be interacting with the portal. Personas include: • Regular users • Service desk	The number of personas will be limited to 5.

	• Account administrators • Distribution group administrators • Security group administrators	
Schema and user interface customizations	• Design and implement the extensions to the MIM schema, including additional attributes per the customer requirements • Design and implement the placement of these attributes in the web forms used to manage users and groups from the MIM Portal	The number of new attributes added to the schema and to the web forms will be limited to 20.
Configure the Oracle Database Connector for connectivity to the HR System	• Design data Import from HR, including delta change detection. • Design data Export to HR • Install and Configure the Generic SQL Connector	Orange County will be responsible for setting up the views, tables, triggers or stored procedures needed by MIM to read and write to the HR database through this connector.
Synchronize user information between AD and HR	• Design and Implement synchronization rules to: o Join the user records imported from HR with the ones imported from AD o Synchronize select attributes from HR to AD o Synchronize select attributes from AD to HR	
User management in AD from HR (Employees)	Design and implement workflows to provision and deprovision user accounts in AD based on the user profile information imported from HR. Workflows include: • Unique account name and random strong password generation • Construction of the DisplayName • Creation of the user account in the right domain and AD organizational unit based on an employee HR attribute. • Notification sent to the manager and Service Desk on successful account creation • On termination from HR, disable the account and move it to the disabled organization unit followed by deletion 90 days later • Upon re-activation, re-enable the user account and move it back to the correct organization unit; if the user	Employee user attributes will be built based on other attributes imported into the MIM service database. The number of user attributes built or validated is limited to 20. Customer will be responsible for providing an HR attribute to AD domain mapping to control to which of the agency domains a user account will be created.

	account has been deleted, re-create the user account in AD.	
User management in AD from MIM Portal (Contractors)	Design and implement workflows to provision and deprovision contractor user accounts in AD based on the user profile information imported from the MIM Portal. Workflows include: • Unique account name and random strong password generation • Construction of the DisplayName • Creation of the user account in the right domain and AD organizational unit based on a contractor department attribute set in the MIM Portal. • Notification sent to the manager and Service Desk on successful account creation • On termination in the MIM Portal, disable the account and move it to the disabled organization unit followed by deletion 90 days later • Upon re-activation in the MIM Portal, re-enable the user account and move it back to the correct organization unit; if the user account has been deleted, re-create the user account in AD.	Contractor user attributes will be built based on other attributes entered the MIM portal through end-user data entry. The number of contractor user attributes built or validated is limited to 20.
User Transfer between departments in different domains	When a user transfers from one department to another and this transfer results in a change of user domain, the following actions will occur: • Actions will occur when the department value is received from HR for employees or from the MIM portal for contractors • When the user department value changes, ○ Disable the account current domain and move it to the disabled organization unit followed by deletion 90 days later ○ Provision a new account in the new domain corresponding to the new department value.	Mail attributes will not be transitioned to the new user. Mailbox management is out of scope. User group memberships will not be preserved. The transfer process results in a new user object whose entitlements must be granted after creation.

	• Notification sent to the new manager and Service Desk of user transfer.	
Entitlement Management in loosely connected systems	• Design and implement workflows to request the provisioning/de-provisioning of user accounts and associated entitlements for up to 5 different systems without using MIM connectors • Based on the user data imported from HR for a new hire, or the entitlement selected for an existing user from the MIM Portal, the following workflows take place: o Email notification is sent to an approver to request for approval of the access requested, o Upon approval, an email notification is sent to the system administrator to request manual provisioning of the user account and associated entitlements • When the user is terminated in HR or from the MIM Portal an email notification is sent to all system administrators to request the deprovisioning of the user access in their respective systems • Optionally the system administrators can be asked to confirm the provisioning or de-provisioning actions they have taken by selecting a checkbox in the user's profile from the MIM Portal. • User self-service will allow users to update their cell phone, fax, and office location in the MIM portal.	
Group management in AD from the MIM Portal	Design and implement the workflows and synchronization rules used to manage security and distribution groups in AD. Workflows include: • Attribute validation and naming convention enforcement • Approval required when joining certain groups • Group owner notification for extending the group prior to expiration and deletion of the group upon expiration	The number of group attributes built or validated is limited to 3. Group owners will be maintained manually by the group administrators. Group size is limited to less than 25,000 members.

Group management in AD from HR	• Design and implement the workflows to automatically generate dynamic groups based on the imported user data, such as a group is automatically created for each city present in the employee records imported from HR. • The membership of these dynamic groups is automatically calculated based on the data imported from HR and AD. • Exceptions to these dynamic group memberships is handled by adding users to corresponding Inclusion or Exclusion manual groups. • Each of these Inclusion and Exclusion groups can be requested from the MIM Portal and automatically created by MIM.	
Dynamic Group conversion	Convert up to 5 groups imported from AD to Dynamic Groups and provide guidance to the Orange County on how to convert the remaining groups	Scope is limited to 5 dynamic groups.
Self-Service Password Reset	Allow the user to update their passwords in a Self-Service Password Reset (SSPR) portal without administrative intervention. The password reset operations will be initiated from Azure AD and flowed down to the target user account domain.	
Bulk Import from a CSV file	Provide a PowerShell script to allow for creating, updating, and deleting user, contact, and group resources in MIM from a CSV file	
High-availability	Plan for high-availability of the different solution components within the overall design	Orange County will be responsible for providing the load balancing solution and for implementing the SQL servers for high-availability.
Test environment	Build the solution in a test environment based on the Functional Specification document	
User acceptance testing (UAT)	Assist the customer stakeholders in conducting UAT in the test environment, based on the documented test cases in the Test Plan	UAT will be limited to 5 days
Production rollout	• Assist Orange County with the implementation of the solution in the production environment based on the Deployment Guide • Import from AD, all user, contact and group objects to be managed from the MIM Portal	Scope is limited to fewer than 50,000 users and 50,000 groups imported from AD.

	- Import from HR all user records and make sure they join with corresponding AD accounts. - Validate the changes resulting from the data imported from HR before exporting them to AD. - Validate the changes resulting from the data imported from AD before exporting them to HR.	The remediation activities required to fix un-joined objects and unwanted changes is time-boxed to 4 days.
Stabilization of the solution in production	- Assist Orange County in performing UAT in production. - Monitor the solution in production to detect and fix any issues that may arise, according to Section 1.2.7: Testing	Stabilization activities in production will be limited to 10 days
Knowledge Transfer	Provide informal knowledge transfer to the customer staff on the solution components implemented.	

1.2.2 Software Products and Technologies

The products listed in the following table are required to deliver this project. Orange County is responsible for obtaining all required licenses and products.

Table 2: Software Products/Technologies Required

Product and Technology Item	Version	Required By Date
SQL Server	2014	Prior to start of project
Microsoft Identity Manager	2016	Prior to start of project

1.2.3 Data Migration

No data migration is expected.

1.2.4 Integration and Interfaces

The implementation of the following MIM Connectors is in scope.

Table 3: Integration Interfaces Scope

Interface Name	Description of Scope	Responsibility
MIM Service	Out-of-the-box connector used to synchronize data between the MIM Service database and the MIM Synchronization database.	Microsoft
Active Directory	Out-of-the-box connector used to synchronize data between the 27 Orange County AD domains and the MIM Synchronization database.	Microsoft

HR	Out-of-box Oracle Database connector used to synchronize data between the Orange County HR system and the MIM Synchronization database.	Microsoft and Customer
OC Profile	Out-of-box Microsoft SQL Server connector used to synchronize data between the Orange County OC Profile system and the MIM Synchronization database.	Microsoft and Customer

1.2.5 Environments

The environments listed in the following table are required to deliver this project. The party listed is responsible for establishing the environment in the location specified, by the time noted.

Table 4: Required Environments

Environment	Location	Responsibility	Ready by
Development and Test	Customer	Customer	One week prior to the start of Build phase
Production	Customer	Customer	One week prior to the start of Deploy phase

The development and test environment must have an instance of AD with similar data as in production. In particular, the following objects need to be the same: Organizational Units, Users, Contacts and Groups.

An instance of the HR system must also be set up in the test environment with data similar to production. Note however that if the Customer cannot setup the HR system but can provide the backend database, then they should provide a script to perform the operations needed during testing.

1.2.6 Training and Knowledge Transfer

Knowledge transfer is defined as informal activities provided when Orange County team members are working side-by-side with Microsoft. These include, but are not limited to, the following: whiteboard discussions, email threads, conference calls and facilitated meetings on technical topics. No deliverables or meeting summary will be provided for these sessions or activities.

Informal knowledge transfer is a valuable adjunct to, but not a substitute for, formal training. Microsoft recommends that formal training be procured and attended by the technical staff prior to the initiation of this project.

1.2.7 Testing

The following testing is in scope.

Table 5: Testing Scope

Test Type	Description	Responsible	Provides Test Data/Cases	Guidance & Support	Environment
Unit testing	Unit test specific functionality of the individual solution components during the Build process.	Microsoft	Microsoft	Microsoft	Development/Test

Functional testing	Functional testing focuses on the functionality of the solution meeting the design and integration with connected data systems. Test cases are based upon the Functional Specification document.	Microsoft	Microsoft	Customer	Development/Test
UAT	Test functionality of key customer real world scenarios. Testing is based on the test plan where test cases with step-by-step instructions are documented.	Customer	Customer	Microsoft	Development/Test; Production

As defects are identified during testing, the defect priority will be jointly agreed upon by the customer and Microsoft. The Microsoft team will triage the defect and fix all in-scope P1 and P2 defects. Defect priorities are shown in the following table.

Table 6: Defect Priorities

Defect Priority	Description of Priority
P1	Showstopper defect. Development, testing, or production launch cannot proceed until the defect is corrected. Must fix as soon as possible. Defect is blocking further progress in this area. Solution cannot ship and the project team cannot achieve the next milestone.
P2	Defect must be fixed prior to moving to production. Does not affect test plan completion
P3	It is important to correct the defect. However, it is possible to move forward into production using a workaround. Does not impact functionality as designed (for example, message change in user experience program).
P4	Feature enhancement or cosmetic defects. Design change from original concepts.

Note: P3 and P4 defects will be logged and the customer may choose to schedule their remediation either by change request, by the Change Management Process described in Section *2.4.4* of this SOW, or during a subsequent release. P3 and P4 defects will not be corrected by default under this SOW.

Note: Product bugs and design change requests are not in scope. Product related issues must be addressed separately through Premier support.

1.3 Areas Out of Scope

Any area that is not explicitly listed in Section 1.2 as within scope is out of scope for this engagement. The areas that are out of scope for this engagement include, but are not limited to, the following:

Table 7: Areas Out of Scope

Area	Description
Integration with additional applications and systems	MIM will be integrated with 27 Active Directory domains, an HR system, and OC Profile database through out-of-box connectors. Five systems of the customer choosing will also be integrated but without connectors, meaning that MIM will only send email notifications to their respective system administrators to perform manual provisioning and deprovisioning. Any other additional systems are out of scope.
Advanced user management	Any operation other than creating, updating, or deleting user and contact objects in AD is not in scope. This includes creating and managing user shares, provisioning Microsoft Exchange mailboxes, or setting user permissions on network resources.
Advanced group management	Advanced group management workflows are not in scope. These include, but are not limited to, the following: • Automatic ownership management • Periodic group attestation • Group nesting • Empty group notification
Exchange resource management	Management of resources such as mailboxes, contacts, and distribution lists in Microsoft Exchange Online or Exchange on-premises. Contacts and distribution lists will be managed only in AD and will not be tested with Exchange as part of this engagement.
MIM reporting	The MIM reporting component will not be installed as part of the solution, meaning that the ability to track historical actions taken and changes made through MIM will be limited to 30 days only.
Management of tier-0 accounts and groups	The management of tier-0 or administrative user accounts and groups.
Data clean-up	Cleaning the data in AD, including making sure that the attributes imported comply with the data format standard in MIM (such as MailNickname, Email and AccountName). This includes the population of the employeeID attribute on all user objects.
Disaster recovery	Implementation of a solution that is geo-resilient.
Custom portal	The development of a custom web portal. Only the default MIM Portal will be customized to the extent of its out-of-box capabilities.
MIM Client Extensions	The deployment of MIM client extensions such as the Outlook add-in to user workstations for request approval or group management.

AD redesign or changes	Any AD redesign or changes to the current AD environment will be the customer responsibility.
SQL infrastructure	Implementation of a highly-available SQL infrastructure used by the solution components will be the customer responsibility.
Networking	Implementation of firewall changes, load balancer setup, or any other form of networking changes will be the customer responsibility.
Hardware	Hardware will not be provided under this SOW. The customer is responsible for acquiring all necessary hardware
Product licenses	Product licenses (Microsoft or non-Microsoft) will not be provided under this SOW. The customer is responsible for acquiring all necessary product licenses required as a result of this SOW.
Process re-engineering	Design of functional business components of the solution unless specifically included in scope and delivered by the Microsoft Consulting Services (MCS) Operations Consulting staff.
Organizational change management	Design or re-design of the customer's functional organization unless specifically included in scope and delivered by MCS Operations Consulting staff.
Formal training	Formal classroom or hands-on lab training.

2 Project Approach, Timeline and Deliverable Acceptance

2.1 Approach

The estimates for this project assume that we will use the Microsoft Solutions Framework (MSF) to implement each phase within this SOW. MSF represents a world-class solution development approach that provides for well-defined phases that take into account definition of requirements, architectural design, detailed solution design, solution build, solution testing, and managed release cycles of the solution.

2.1.1 Engagement Initiation

Successful delivery and adherence to the schedule defined in this section requires the customer to complete the following prior to project kickoff:

- Identify all stakeholders who may have an interest in the project and make sure that they are invited to the kick-off meeting.
- Collect any documentation that may be helpful during the delivery, such as:
  - Business and Technical Requirements, such as:
    - Security policies and standards
    - Standards for server configuration
    - Naming convention for users and groups stored in AD

- Current Identity and Access Management solution information, including the processes used.
- AD design documentation such as forests, domains, trusts, sites, group policies, and organizational units (OUs)
- Network diagrams, indicating at a minimum the different local-area networks (LANs), wide-area network (WAN) links, available bandwidth, and any firewall or packet filtering devices
- Operations information, such as:
  - Backup and restore standards and infrastructure documentation
  - System-monitoring standards and documentation
  - Change Management processes and tools
- HR data information, such as thc attributes present in the HR database and sample data for each. A dump of the HR data in a CSV file is usually very helpful.

2.1.2 Envision Phase

During the Envision phase, the team will define the requirements for the overall solution, gain an understanding of the environment, design a high-level solution stratcgy that meets the requirements, and define the roles and responsibilities of the project team. The Microsoft tcam will create a Vision and Scope document to identify what will be accomplished and align expectations between the project team and stakeholders. The Envision Phase ends when the Vision and Scope document is approved by Orange County. This milestone indicates that the team shares a common vision and agrees on the scope of work necessary to bring the vision to reality.

Table 8: Envision Phase

Category	Description
Microsoft activities	▪ Project kick-off meeting. ▪ Review existing documentation. ▪ Conduct Envisioning and Assessment workshops. ▪ Discover the current identity and access management processes. ▪ Review the AD structure and how user, contact and group objects are stored in each of the 27 in-scope Active Directory domains. ▪ Review data attributes which will be pushed to the OCProfile database. ▪ Review current processes for maintaining users in HR. ▪ Review the schema of the HR database and the user profile information maintained. ▪ Collect customer business and technical requirements. ▪ Validate the project vision statement and project goals. ▪ Determine the personas interacting with the solution. ▪ Define the identity management use cases. ▪ Document the results and findings collected from various stakeholders in the Vision and Scope document.
Customer responsibilities	▪ Coordinate resources for participation in the Envisioning and Assessment workshops. ▪ Facilitate any necessary communication for requests that may result from discussions during the Envisioning and Assessment workshops, including information-gathering exercises. ▪ Make available all documentation that may be helpful to the project.

	▪ Provide all necessary information regarding the existing environment and the systems that are in scope. ▪ Participate in the review and approval process of the Vision and Scope document. ▪ Procure the necessary hardware or virtual machines for the development/test environment.
Exit criteria	▪ Approval of the Vision and Scope document.
Key assumptions	▪ Orange County stakeholders will be available on a part-time basis to attend the Envisioning and Assessment workshops, answer Microsoft questions, and validate the solution requirements and use cases. ▪ During this phase, the team will gather additional information needed for refinement of the in-scope solution. This information will be used during the Plan Phase to complete the solution architecture design. ▪ The Vision and Scope document will be written using Microsoft Services templates.

Workshops

With customer participation, the following workshops will be led by Microsoft during this phase.

Table 9: Workshops

Activity	Topics Covered	Maximum Hours per Session	Maximum Number of Sessions
Envisioning and Assessment workshops	▪ Review the current AD environment ▪ Discuss how identities are stored and managed in the 27 in-scope Active Directory domains. ▪ Discuss how the OCProfile will be transitioned to a consumer of data from MIM. ▪ Discuss HR onboarding/offboarding processes ▪ Discuss how employee information is stored and managed in HR. ▪ Collect detailed customer requirements for the in-scope identity management processes. ▪ Discuss MIM product capabilities. ▪ Outline conceptual future state. ▪ Discuss other initiatives related to the project.	2	5
Document review	▪ Review Vision and Scope document	2	1

Phase Outputs

The customer will provide the following items:

Table 10: Phase Outputs

Name	Description
Decisions	▪ Validation of the scope, requirements, and use cases for the project

Development and Test Lab	▪ Hardware and software for the Development /Test lab environment.

Microsoft will provide the following Service Deliverables. Those that require formal review and acceptance, as described in Section *2.3* Service Deliverable Acceptance Process, are indicated as such.

Table 11: Envision Phase Service Deliverables

Name	Description	Acceptance Required (Y/N)
Vision and Scope document	Contains a description of the customer's situation and needs, the boundary of the solution defined though the range of features and functions, and the solution design strategy that will form the starting point used to create the customer's solution. Designs at this stage will be conceptual in nature and will provide input to developing the functional specification. This document includes the project vision, all agreed upon requirements, and a solution design approach.	Y

2.1.3 Plan Phase

During the Plan Phase, the team works through the design and prepares the Functional Specification document and Project Plan. Following the completion of this phase, the team begins the development of the solution in the Build Phase.

Table 12: Plan Phase

Category	Description
Microsoft activities	▪ Facilitate solution design sessions to define how MIM will implement the use cases documented in the Vision and Scope document. ▪ Discuss different options with the customer database administrators for how to read or write user data to the HR database. ▪ Document the logical and physical design of the solution components in the Functional Specification document ▪ Assist the customer Project Manager in the creation of the Project Plan. ▪ Review the Test lab to make sure it meets the requirements for the project.
Customer responsibilities	▪ Coordinate resources for participation in design sessions. ▪ Make timely decisions about specific design elements. ▪ Create the communications and training plan for the project. ▪ Participate in the review and approval process of the Functional Specification document. ▪ Work with Microsoft resources to create and maintain a Project Plan (work breakdown structure) document. ▪ Review and approve the Functional Specification document. ▪ Setup AD in the development/test environment with similar data as in production. In particular, the following objects need to be the same: Organizational Units, Users, Contacts and Groups. ▪ Setup the HR system in the development/test environment with similar data as in production.

Exit criteria	▪ Approval of the Functional Specification document
Key assumptions	▪ Orange County will provide necessary technical subject matter experts who will make design decisions. ▪ The AD forest setup in the Development/Test Lab contains the same domains, organizational unit structure, users, contacts and groups as the one in production. ▪ The HR database setup in the Development/Test Lab contains the same user and department information as in production. ▪ Orange County will be responsible for setting up the views, tables, triggers or stored procedures needed by MIM to read and write to the HR database through this connector. ▪ The Functional Specification document will be written using Microsoft Services templates. ▪ The Project Plan will be in a Work Breakdown Structure (WBS) format using Microsoft Project.

Workshops

With Customer participation, the following workshops will be led by Microsoft during this phase.

Table 13: Workshops

Activity	Topics Covered	Maximum Hours per Session	Maximum Number of Sessions
Design workshops	▪ Discuss initial user and group import from AD. ▪ Discuss user management in AD from the MIM Portal. ▪ Discuss group management in AD from the MIM Portal ▪ Discuss how user and department information will be imported from HR for employees, including delta change detection out of the HR database. ▪ Discuss how user and department information will be imported from the MIM Portal for contractors. ▪ Discuss how user attributes will be written to HR. ▪ Discuss how the current 12 attributes synchronized to in-scope directories by Unity Sync will be transitioned to MIM.	2	5
Document review	▪ Functional Specification document	2	1

Phase Outputs

The customer will provide the following items:

Table 14: Phase Outputs

Name	Description
Decisions	▪ Make decisions relative to the design of the proposed solution
Development and Test Lab	▪ The Development and Test Lab has been setup by Orange County per Microsoft's requirements and is ready for MIM installation.

Microsoft will provide the following Service Deliverables. Those that require formal review and acceptance, as described in Section *2.3* Service Deliverable Acceptance Process, are indicated as such.

Table 15: Plan Phase Service Deliverables

Name	Description	Acceptance Required (Y/N)
Functional Specification document	Contains the specification of the logical and physical design for the different components of the proposed solution. This document includes the details of all the configuration settings for the solution components. Someone with MIM skills should be able to reconfigure the solution from scratch using this document.	Y

2.1.4 Build Phase

During the Build Phase, the team refines the baseline design created in the Plan Phase, builds the solution functionalities, and performs unit testing of each use case implemented. Completion of this phase marks the transition to the Stabilize Phase.

Table 16: Build Phase

Category	Description
Microsoft activities	▪ Install MIM in the Development/Test Lab. ▪ Configure the management agent and synchronization rules for the MIM Service connector. ▪ Configure the management agent and synchronization rules for the AD connectors to the 27 in scope Active Directory forests. ▪ Configure the management agent and synchronization rules for the Generic SQL connector used for HR connectivity. ▪ Configure the management agent and synchronization rules for the SQL Server connector used for OCProfile connectivity. ▪ Configure the Sets, Workflows, and Management Policy Rules (MPRs) to model the identity management processes based on the requirements and use cases documented in the Vision & Scope document. ▪ Customize the MIM Portal. ▪ Conduct unit testing, fix issues found, and retest solution components. ▪ Draft the Test Plan describing the test environment and containing all test cases required to validate the requirements and use cases documented in the Vision & Scope document. ▪ Develop the Deployment Guide document.
Customer responsibilities	▪ Coordinate resources for participation in the Build activities. ▪ Setup the tables, views, triggers or stored procedures as requested by Microsoft for the HR Generic SQL Connector. ▪ Assist with the definition of the test cases for the solution. ▪ Review and approve the Test Plan document. ▪ Review and approve the Deployment Guide document.
Exit criteria	▪ Solution is built and prepared for testing. ▪ Approval of the Deployment Guide document ▪ Approval of the Test Plan document

Key assumptions	▪ The Microsoft team will have access to user accounts that are granted administrative privileges on all servers where the solution components are installed in the Development/Test Lab. ▪ The Test Plan and Deployment Guide documents will be written using Microsoft Services templates.

Phase Outputs

Microsoft will provide the following Service Deliverables. Those that require formal review and acceptance, as described in Section *2.3* Service Deliverable Acceptance Process, are indicated as such.

Table 17: Build Phase Service Deliverables

Name	Description	Acceptance Required (Y/N)
Deployment Guide document	This document describes the steps to install and configure MIM in the production environment.	Y
Draft Test Plan	A draft document that describes test objectives, test methodologies and tools, expected results, responsibilities, and resource requirements. It details all test cases for the solution and is provided in draft format until the test cases have been implemented during the Stabilize Phase.	Y

2.1.5 Stabilize Phase

During the Stabilize Phase, the team conducts testing and focuses on resolving issues and bugs to prepare the solution for release. Completion of this phase marks the transition to the Deploy Phase.

Table 18: Stabilize Phase

Category	Description
Microsoft activities	▪ Perform functional testing of the solution built in the test environment. ▪ Adjust solution design and configuration settings as appropriate. ▪ Assist customer in the completion of UAT per the test cases documented in the test plan. ▪ Update the test plan document based on actual results of the testing. ▪ Conduct knowledge transfer about the solution built to the customer.
Customer responsibilities	▪ Begin scheduling for the production deployment. ▪ Provide staff to assist with UAT testing of the solution. ▪ Conduct UAT and provide test results to the Microsoft team. ▪ Review and approve the test plan updated with the test results.
Exit criteria	▪ Acceptance of the test results from the Test Plan, authorizing the deployment of the solution into the production environment.
Key assumptions	▪ Orange County will perform all UAT activities and Microsoft will provide assistance as needed.

Phase Outputs

The customer will provide the following items:

Table 19: Phase Outputs

Name	Description
Test results	Test results at the completion of UAT.

Microsoft will provide the following Service Deliverables. Those that require formal review and acceptance, as described in Section 2.3 Service Deliverable Acceptance Process, are indicated as such.

Table 20: Stabilize Phase Service Deliverables

Name	Description	Acceptance Required (Y/N)
Final Test Plan	The final test plan includes all the test results and notes that were captured for each test case executed during UAT. This document is used as an approval mechanism for implementing the solution into the production environment.	Y

2.1.6 Deploy Phase

During the Deploy Phase, the team conducts the activities needed to deliver the solution in the production environment. The Deploy Phase includes the monitoring and stabilization of the solution while transitioning it to the operations and support teams before project close out.

Table 21: Deploy Phase

Category	Description
Microsoft Activities	▪ Conduct a one-hour Assessment Workshop to assess Orange County readiness to operate and maintain the solution in production. ▪ Assist Orange County with the deployment of the solution to production per the Deployment Guide. ▪ Initially import and aggregate the data from HR and AD into MIM. ▪ Remediate the un-joined objects and the unwanted changes before exporting the changes to AD or HR. Note that this activity is time boxed to 3 days. ▪ Assist Orange County in conducting UAT in production. ▪ Monitor, troubleshoot, and fix issues that result from the use of the solution in the production environment. ▪ Update the Functional Specification document with the final design and configuration settings. ▪ Conduct a project close-out meeting to wrap up the engagement and share lessons learned.
Customer Responsibilities	▪ Participate in the Assessment Workshop and confirm that the solution is ready for deployment. ▪ Provide relevant personnel needed for deployment, operations, and support. ▪ Participate in the project close-out meeting.
Exit Criteria	▪ Acceptance of the test results from the test plan completed in production.
Key Assumptions	▪ Stabilization activities in production is limited to 8 business days.

2.2 Timeline

It is estimated that this engagement will be performed over a duration of 50 weeks from the start date of August 5th 2019. The actual timeline for this engagement will be relative to the project start date, and all dates and durations provided are estimates only.

Figure 1: Project Timeline

2.3 Service Deliverable Acceptance Process

At specified milestones throughout the project, Microsoft will submit completed project service deliverables for customer's review and approval. Service deliverables will fall into the following categories:

1. Document deliverables (for example, Word, Excel, Visio, or Project).
2. Functioning components or solution deliverables (such as custom source code).

The customer's use or partial use of a service deliverable will constitute acceptance of that Service Deliverable. The customer may provide its acceptance or rejection of deliverables electronically through email. The following details the acceptance process for each of the deliverable types.
Document deliverables: within three business days from the date of submittal, the customer must either:

- Accept the document deliverable by signing, dating, and returning the Service Deliverable Acceptance Form
  OR
- Provide a written notice rejecting the document deliverable, including a single and complete list describing every reason for rejection.

The following assumptions also apply:

- Document deliverables shall be deemed accepted unless customer provides a timely, written rejection notice as described previously.
- Microsoft will correct problems with a document deliverable that are identified in the written rejection notice, as described above, and within the scope of this SOW, after which the document deliverable will be deemed accepted.
- Issues that are outside the scope of this SOW and feedback provided after a document deliverable has been deemed accepted will be addressed as a potential change of scope pursuant to the Change Management Process outlined in this SOW.

Functioning components or solution deliverables: the functioning solution is typically comprised of configured commercial software and custom source code and associated objects. Review and acceptance of the solution or custom source code, for this SOW only, is based on completion and signoff of the defined customer acceptance test.

2.4 Project Governance Approach

This section outlines the project governance structure and processes to which the Microsoft team will adhere for this engagement.

2.4.1 Part-Time Project Management

This project will be managed by a part-time Project Manager based on a commitment of up to **8 hours** per week. Prior to the start of the engagement, a mutually agreed to coverage plan or meeting schedule will be documented in writing. As this resource is part-time, the following operational constraints are assumed:

Table 22: Project Management Activities

Activity	Description
Communications	▪ Provide one weekly status report. ▪ Prepare and lead one status meeting per week of no more than one hour in duration. ▪ Remotely attend or participate in one steering committee meeting per month. Note: not all customer meetings will be attended.
Scope management and change control	▪ Attend one scope meeting per week remotely. ▪ Manage project change control.
Finance	▪ Provide weekly financial report as part of the weekly status report.
Schedule	▪ Manage the schedule for the MCS scope of work and MCS resources.
Human resources and staff management	▪ Coordinate MCS resources (only), including staffing, task assignments, and status reporting.

The scope of the Microsoft part-time project management service is limited to managing MCS and Microsoft partners who are subcontracted through MCS.

Microsoft will provide project management for the duration that is defined in the Work Order. Changes to this duration or to the amount of hours per week will be handled by the change management process.

2.4.2 Communication Plan

The following will be used to provide formal communication during the course of the project:

- The Microsoft Project Manager, working in conjunction with the customer Project Manager, will document a detailed communication plan as part of the master project management plan and will compile weekly status reports for distribution to both customer and Microsoft management.
- Weekly status meetings will be held to review the project's overall status, the acceptance of deliverables, the project schedule, and open issues noted in the status report.

2.4.3 Issue/Risk Management Procedure

The following general procedure will be used to manage active project issues and risks during the project:

- **Identify**: Identify and document project issues (current problems) and risks (potential events that impact the project)
- **Analyze and prioritize**: Assess the impact and determine the highest priority risks and issues that will be managed actively

- **Plan and schedule**: Decide how high-priority risks are to be managed and assign responsibility for risk management and issue resolution
- **Track and report**: Monitor and report the status of risks and issues and communicate issue resolutions
- **Control:** Review the effectiveness of the risk and issue management actions

Active issues and risks will be monitored and reassessed on a weekly basis.

2.4.4 Change Management Process

During the project, either party may request in writing additions, deletions, or modifications to the services described in this SOW ("change request").

For all change requests, regardless of origin, Microsoft will submit to the customer the Microsoft standard Change Request Form, which will describe the proposed changes to the project, including the impact of the changes on the project scope, schedule, fees, and expenses.

For all change requests originated by the customer, Microsoft will have a minimum of 3 business days from receipt of the change request to research and document the proposed change and prepare the Change Request Form.

The customer will have 3 business days from your receipt of a completed Change Request Form to accept the proposed changes by signing and returning the Change Request Form. If the customer does not sign and return the Change Request Form within this time period, the change request will be deemed rejected and Microsoft will not perform the proposed changes.

No change to this project will be made unless it is requested and accepted in accordance with the process described in this section. Microsoft will have no obligation to perform or commence work in connection with any proposed change until a Change Request Form is approved and signed by the designated project managers from both parties.

2.4.5 Executive steering committee

The executive steering committee provides overall senior management oversight and strategic direction for the project. The executive steering committee for the project will meet per the frequency defined in the communication plan and will include the roles listed in the following table. The responsibilities for the committee include:

- Making decisions about project strategic direction.
- Serving as a final arbiter of project problems.
- Approving significant change requests.

Role	Customer
Project sponsor	Customer
Delivery manager	Microsoft

2.4.6 Escalation path

The Microsoft project manager will work closely with the Customer project manager, sponsor, and other designees to manage project problems, risks, and change requests as described previously. The Customer will provide reasonable access to the sponsor or sponsors in order to expedite resolution. The standard escalation path for review, approval, or dispute resolution is as follows:

- Project team member (Microsoft or the Customer)
- Project manager (Microsoft and the Customer)
- Executive steering committee

2.5 Project Completion

Microsoft will provide services defined in this SOW to the extent of the fees available and the period of performance specified in the Work Order. If additional services are required, the Change management process will be followed, and the contract modified. The program will be considered complete when at least one of the following conditions has been met:

- All fees available have been utilized for services delivered and expenses incurred.
- The term of the program has expired.
- All Microsoft activities and in-scope items have been completed.
- The Work Order has been terminated.

3 Project Organization and Staffing

3.1 Project Organization Structure

This section describes the overall project organization structure, reporting relationships, and key project roles.

The project will be organized as depicted in the following diagram.

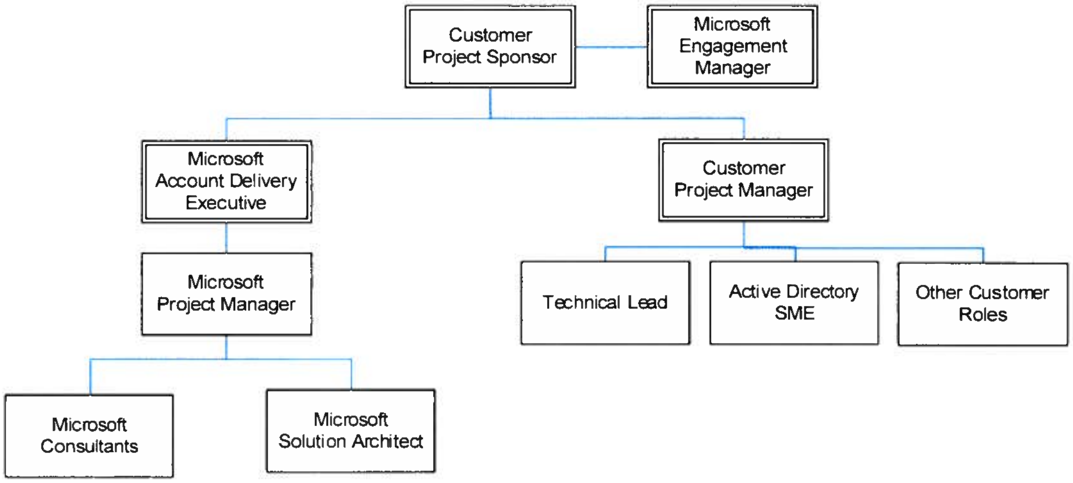


Figure 2: Project Organization Structure

3.2 Project Roles and Responsibilities

This section provides a brief description of key project roles and responsibilities.

3.2.1 Customer Project Roles and Responsibilities

Table 23: Customer Roles and Responsibilities

Role	Responsibilities	Project Commitment
Customer Project Sponsor	▪ Makes key project decisions, serves as a point of escalation, and clears project roadblocks.	Part-time
Customer Project Manager	▪ Primary point of contact for Microsoft team. ▪ Responsible for managing and coordinating the overall project and delivering to schedule. ▪ Responsible for customer resource allocation, risk management, project priorities, and communication to executive management. ▪ Coordinates decisions within three business days, or otherwise agreed timeline.	Part-time
Technical Lead	▪ Primary technical point of contact for the team that is responsible for technical architecture and identity management processes.	Part-time
AD Subject Matter Expert (SME)	▪ A SME on the current AD implementation at Update [Customer Name] in Doc Properties.	Part-time
Other customer roles	▪ Other stakeholder from Orange County working with the Microsoft team to provide information about the current environment and express their requirements for the project.	Part-time

3.2.2 Microsoft Project Roles and Responsibilities

Table 24: Microsoft Roles and Responsibilities

Role	Responsibilities	Project Commitment
Account Delivery Executive	• Responsible for managing and coordinating the overall Microsoft project • Single point of contact for escalations, billing issues, personnel matters, contract extensions • Facilitates project governance activities, leading the Executive Steering Committee	Part-time
Project Manager	• Responsible for managing and coordinating the Microsoft project delivery	Part-time

	• Responsible for issue and risk management, change management, project priorities, and weekly status communication and weekly status meeting • Coordinates only MCS resources and partners subcontracted to MCS, including staffing, task assignments and status reporting	
Solution Architect	▪ Responsible for overall solution design ▪ Provides technical oversight. ▪ Verifies that Microsoft recommended practices are followed. ▪ Sets operational criteria for release to production.	Part-time
Consultant	▪ Assists with the solution design. ▪ Builds and configure the solution components. ▪ Performs unit and functional testing. ▪ Assists customer in performing UAT and deploying the solution to production. ▪ Conducts knowledge transfer. ▪ Produces all project deliverables.	Full-time

4 General Customer Responsibilities and Project Assumptions

4.1 General Customer Responsibilities

Delivery of Microsoft services depends upon the following customer responsibilities, among other items:

- The customer will provide suitable work spaces with desks, chairs, telephones.
- The customer will provide LAN connections giving the Microsoft onsite team access to the Internet and email.
- The customer will provide access to all necessary customer work sites, systems logon, passwords, and material and resources as needed and as advised by us in advance.
- The customer will assume responsibility for management of all non-Microsoft managed vendors.
- The customer will provide access with proper licenses to all necessary tools and third-party products required for Microsoft to complete its assigned tasks.
- The customer will acquire and install the appropriate server capacity required to support the environments as defined in the scope section of this SOW.
- The customer will provide accurate and complete information, as needed.
- The customer will take timely decisions and obtain approvals from management, as needed.
- The customer will provide Project Management.

4.2 Project Assumptions

The Services, fees, and delivery schedule for this project are based on the following assumptions:

1. The standard work day for the project is between 8:00 AM and 5:00 PM local time where the team is working, Monday through Friday, except for scheduled holidays.
2. In performing services under this SOW and the applicable Work Order, Microsoft will rely upon any instructions, authorizations, approvals, or other information provided by the customer's Project Manager or personnel duly designated by the customer's Project Manager. All estimates regarding fees, timelines, and our detailed solution are based on information provided by the customer to date.
3. Microsoft resources and Microsoft subcontractors' resources may perform services remotely or onsite from Microsoft facilities, customer facilities, or Microsoft partner's facilities.
4. Informal knowledge transfer will be provided throughout the project. Informal knowledge transfer is defined as the customer's staff working alongside Microsoft staff. No formal training materials will be developed or delivered as part of informal knowledge transfer.
5. If the project schedule requires Microsoft resources or Microsoft subcontractors' resources to perform dedicated services at the customer's site on a weekly basis, Microsoft resources will typically be onsite for three nights and four days; arriving on Mondays and leaving on Thursdays.

4.2.1 Solution Specific Assumptions

The following list of assumptions apply to this project and are specific to the solution being implemented:

1. Customer stakeholders will review and sign off on each document within three business days. If sign-off and document revisions are not received within three business days, Microsoft will assume approval with no revisions and will proceed with project activities. Microsoft will attempt to incorporate later revisions if received and will attempt to minimize impact to the project timeline, but revisions outside of the three business day review period may result in an increased project duration and additional fees charged to accommodate re-work.
2. Prior to the start of the Build phase the customer must have set up a test environment with an instance of Active Directory that has similar data as in production. In particular, the following objects need to be the same: Organizational Units, Users, Contacts and Groups.
3. Up to two "MIM Service" and one "MIM Synchronization Service" components will be implemented in each one of the two environments: Development/Test and Production.
4. Only one Active Directory forest is in scope and the number of domains is limited to four.
5. There will be fewer than 50,000 users and 50,000 groups imported into MIM. The largest group will have fewer than 25,000 members.
6. The number of new attributes added to the schema and to the web forms will be limited to 20.
7. Fewer than five groups will be converted to Dynamic Groups, however, the procedure for converting additional ones will be provided.
8. Customer will setup the load balancers and configure SQL clustering to allow for the deployment of MIM components in a Highly Available configuration.
9. Knowledge transfer will be provided and will consist of the customer's resources working side by side with Microsoft resources to understand the solution implemented. No custom training materials will be developed, and no formal training will be provided.
10. After the initial import from Active Directory, any change made directly to the users, contacts and groups in Active Directory will get overwritten by MIM.
11. Prior to the start of the Build phase the customer must have set up an instance of their HR application and its back-end database in their development/test environment. This database must mirror the one in

production. Note that if the HR application cannot be installed in the development/test environment, the customer should instead provide scripts to directly add/update/delete records in the HR database for testing purpose.

12. Data remediation activities in MIM related to un-joined objects and unwanted changes in Active Directory resulting from the integration with HR are limited to 5 business days.
13. The Project Manager assigned by Orange County to the project must fulfill the following responsibilities:
    - Act as the point of contact for Microsoft with all the Agencies stakeholders
    - Manage all expectations from the Agencies
    - Coordinate decision making across all agencies
    - Align all Agencies with the decisions made in this project
    - Take care of all communications with the leadership and end-users within the Agencies
    - Make sure that the change processes and approvals required within each agency will not delay the deployment during the different phases of the project
    - Any information requested by the Microsoft team must be submitted to the County at a minimum 3 business days in advance. The target completion date for each request must be evaluated against the overall project schedule and reviewed with and agreed by the County. The County will make its best effort to meet the project schedule.
    - Make sure that the technical resource that the delivery team needs to talk to are available within 2 days where possible
    - Make sure that the right resources with decision authority are included in the discussions and if unable to make a decision to meet the project timeline, the Project Manager will have the ultimate responsibility to arrive at a decision.
14. All requests by the delivery team for decisions by Orange County must be submitted at a minimum 3 days in advance. The target completion date for each decision must be evaluated against the overall project schedule and reviewed with and agreed by the County. The County will do its best effort to meet the project schedule.
15. Microsoft will provide a detailed project plan with detailed expected tasks from the County at least 2 weeks in advance of the required date. In unforeseen cases Microsoft may request for information or decisions from the County. If the County does not estimate they can fulfill Microsoft requests within 3 business days they will notify Microsoft within 1 business day and the request will get escalated to the Steering Committee. Any delay may have an impact on the project schedule or the scope of the project and may result in a Change Request.
16. In order to meet the timeline set for this project and simplify the solution, it is critical that all agencies adopt the identity lifecycle management processes outlined in the Vision & Scope document. Any exception will be reviewed to assess impact on the timeline.
17. Orange County is responsible for carrying out the Active Directory cleanup and remediation activities identified in the Vision & Scope document for all agencies. Any agency whose AD data has not been remediated, will be reviewed for impact and decision, which may result in not integrating the agency data with MIM.
18. Orange County is responsible for changing the current HR process and exposing their HR data to MIM in the format detailed in the Vision & Scope document before MIM integration activities with HR can begin.
19. This project assumes a phased rollout as explained in the Vision & Scope document. This is required because each phase builds on each other and this allows us to minimize deployment risks and show value quicker to the stakeholders.
20. It is very likely that most attributes imported from HR will change in AD once the new identity management synchronization rules defined in MIM are enforced. This may include changes such as users being disabled or moved across domains. Microsoft will generate a report containing all the changes for each user in AD prior to the initial export to each domain. It will be the responsibility of each agency to

look at those reports and sign-off on the changes within 3 business days or as mutually agreed and identified in the project schedule. Any delay in this review process will have a significant impact on the project timeline as there are 18 agencies in the scope of this project.

21. Changes requested by an Agency that do not follow the Usage Scenarios outlined in the Vision & Scope document or that will cause a change in the data or the process for other agencies, will be reviewed for impact and decision, which may result in not integrating the agency data with MIM. It is not Microsoft's responsibility to convince the agencies to adopt a single standard for all attributes or to follow the same identity management processes across all the agencies.
22. All testing for each agency before the rollout of each one of the 4 phases of the project, will be planned by the delivery team and reviewed with the County at a minimum two weeks in advance and may be limited to 3 days per phase. It is critical that the Orange County project manager ensures full participation from the agency stakeholders during that period. Failure to do so will have a significant impact on the project timeline. Note that the SOW time-boxes UAT activities for the entire project to 10 days across all 18 forests combined.
23. Orange County must assign a MIM administrator to the project prior to the start of testing for phase 1. This is to allow the Microsoft team enough time to properly ramp up this person on the solution and have her or him help with the User Acceptance Testing (UAT). Otherwise no one will be able to support the solution after the 14 days allocated in the SOW for stabilization activities after production rollout.
24. To ensure the best use of everyone's time during the delivery, all work will be carried out remotely by the Microsoft delivery time. The Microsoft Project Manager, Account Delivery Executive and Architect may still go onsite to coordinate the activities of the remote team.
25. Orange County will provide the Microsoft delivery team Read access to all the Active Directory domains in production at the beginning of the design phase of the project so that the data can be analyzed to develop the identity management rules for MIM.
26. Orange County to provide a Test environment that includes a subset of the current Active Directory domains with data that is a good representation of what MIM will be managing in production. A SQL database containing the full HR data that MIM will be importing must also be provided in this environment. This test environment must be available to the delivery team prior to the end of the Design phase.

    Orange County to also provide connectivity from the on-premise test environment to a test Azure AD tenant.
27. Orange County is responsible for conducting all the Active Directory Environment Remediation activities outlined in the Vision & Scope document prior to the implementation of Azure AD Self-Service Password Reset (SSPR).

ATTACHMENT C

COMPENSATION AND PAYMENT

I. **Compensation:** Microsoft agrees to provide services at the fixed rates and prices as set forth in the Master Agreement. The total amount of this Subordinate Agreement shall not exceed **$529,709.00**. The amount of $529,709 is inclusive of the original total $489,709 plus the amended amount of $40,000 per Amendment No. 1. The County shall have no obligation to pay any sum in excess of this amount unless authorized by written amendment signed by both Parties.

Microsoft shall bill County for goods and services provided according to the rates listed below:

AGREEMENT NOT TO EXCEED TOTAL AMOUNT $529,709.00

Classification/Title	Unit	Published Hourly Rates	Fully-Burdened Rates*
Architectural Consultant	Hour	$305.00	$344.00
Principal Consultant	Hour	$292.00	$331.00
Senior Consultant	Hour	$279.00	$335.00
Project Manager	Hour	$268.00	$307.00
Account Delivery Executive*	Hour	$268.00	$307.00
Consultant*	Hour	$250.00	$308.00
Associate Consultant	Hour	$217.00	$277.00
Technician V	Hour	$260.00	$310.00
Technician IV	Hour	$245.00	$295.00
Technician III	Hour	$216.00	$266.00
Technician II	Hour	$189.00	$239.00
Technician I	Hour	$163.00	$186.00
Technician	Hour	$136.00	$158.00
Offshore Global Delivery Consultant	Hour	$75.00	$75.00
Offshore Global Delivery Project Manager**	Hour	$82.00	$82.00

*The totals referenced above were calculated using fully burdened rates for Microsoft Resources. The services component of these fully burdened rates is equal to "Published Hourly Rates" from Microsoft's Public Sector Services Published Price List for FY18. These fully burdened rates, provided at Orange
County's request, are in compliance with all of its procurement policies, laws, rules and regulations. Fully Burdened Rates include travel expenses.

**The totals referenced above were calculated using Microsoft's Public Sector Services Published Price List for FY20.

II. Payment Workstreams: The engagement has been broken down into four (4) workstreams (see OC MIM Implementation Project Plan V1):

- Workstream 1 - GAL Sync
- Workstream 2 - Azure SSPR
- Workstream 3 - User and Group Management from MIM Portal
- Workstream 4 - HR integration and Provisioning

Per Amendment No. 1, the funding will be allocated according to the following workstreams.

Workstream	Funding Allocation	Acceptance
Workstream 1 - GAL Sync,	Up to max of 15% Contract Value* (up to $79,456.35)	Workstream Signoff
Workstream 2 - Azure SSPR,	Up to a max of 50% Contact Value* (Workstream 1 and 2 cumulative up to $264,854.50)	Workstream Signoff
Workstream 3 - User and Group Management from MIM Portal	Up to a max of 80% Contract Value* (Workstream 1 thru 3 cumulative up to $423,767.20)	Workstream Signoff
Workstream 4 - HR integration and Provisioning	100% Contract Value* (Workstream 1 thru 4 cumulative up to $529,709)	Workstream Signoff

*Contract value is defined $529,709 and does not include Microsoft gratuitous funding.

Payment Terms: Payment shall be made in arrears. Payment will be net forty-five (45) days after receipt of an invoice in a format acceptable to the County of Orange. County shall be billed on a monthly basis and shall be verified and approved by the County subject to routine processing requirements. At the sole discretion of the County, the County may request additional information/clarification from Microsoft in order to obtain sufficient information to process each invoice. The responsibility for providing an acceptable invoice to the County for payment rests with Microsoft. Incomplete or incorrect invoices are not acceptable and will be returned to Microsoft for correction.Billing shall cover goods and services not previously invoiced. Microsoft shall reimburse the County of Orange for any monies paid to Microsoft for good and services not provided or when goods and services do not meet the Agreement requirements. County reserves the right to terminate this Agreement for cause if Microsoft does not meet the applicable specification for the Scope of Work identified in Attachment B.

Payments made by the County shall not preclude the right of the County from thereafter disputing any goods involved or billed under this Agreement and shall not be construed as acceptance of any part of the goods.

III. Invoice Instructions: Each invoice must be on Microsoft's letterhead and have a unique number and shall include the following information:

a. Microsoft's name and address
b. Microsoft's remittance address
c. County Agreement #MA-017-19010780
d. Microsoft's Federal I.D. number
e. Date of Order/Service date(s)

f. Product/service description, quantity, prices

g. Total invoice amount Invoices are to be forwarded to:

County of Orange
OCIT/Budget & Finance Division
Attention: Accounts Payable
1055 N. Main Street, 6th Floor Santa Ana, CA 92701

h. Resource Classification

i. Hourly Rate

j. # of Hours

k. Total (for each Resource Classification)

l. Identify which Workstream the cost is associated with

Microsoft Master Services Agreement

State and Local Government & Public Educational Institutions

Agreement Number **MA-017-19010780**

This Microsoft Master Services Agreement ("Agreement") is entered into between the following entities as of the Effective Date identified below. This Agreement is comprised of this cover page and the attached terms and conditions, Attachments A (County Terms and Conditions), B (Scope of Work), C (Compensation and Payment), D (Microsoft Business Associate Agreement), E (Cybersecurity Best Practices Manual), F (Information Technology Usage), and G (IT Security Policy 2009), the terms of which are incorporated herein by this reference.

This Agreement contains terms of the relationship between County (the entity signing the Agreement and its Affiliates) and Microsoft Corporation (the Microsoft Affiliate signing below and its Affiliates). If County contracts for Professional Services from Microsoft under this Agreement, the specific terms of those transactions included in Attachments A-G is contained in this Agreement and are incorporated by reference herein.

This Agreement or the Statement of Services is not binding on the County until signed by Deputy Purchasing Agent authorized to sign by the Board of Supervisors of County of Orange. By signing below, each party acknowledges that it has read and understood the terms of this Agreement and agrees to be bound by these terms.

County	*Microsoft Affiliate*
Name of County (please print) County of Orange-OCIT	Name **Microsoft Corporation**
Signature Annie Pham	Signature DocuSigned by: David T. Gallagher C5F4FFFE6A2E45D...
Name of person signing (please print) Annie Pham	Name of person signing (please print) David T. Gallagher
Title of person signing (please print) Procurement Contract Specialist	Title of person signing (please print) Director of Contracts
Signature date 5/9/19	Signature date (may be different than Effective Date) 4/15/2019
	Effective Date (may be different than Signature Date) 5/15/19

Contact information. Each party will notify the other in writing if any of the information in the following table changes. The * indicates required fields. By providing contact information, County consents to its use for purposes of administering this Agreement by Microsoft, Microsoft's Affiliates, and other parties that help Microsoft administer this Agreement.

County		
Name of County * County of Orange - OCIT		Contact Name*(This person receives notices under this Agreement pursuant to Article 24 (Notices) in Attachment A). Annie Pham
Street Address* 1055 N. Main Street, 6th Floor, Santa Ana, CA 92701		Contact Email Address* Annie.Pham@ocit.ocgov.com
City* Santa Ana	State CA	Phone 714-567-7409
Country* USA	Postal Code 92705	Fax 714-796-8363
Microsoft		
Notices to Microsoft should be sent to (*Microsoft Affiliate to complete*): * Kevin Hartley, Esq. Microsoft Corporation 5404 Wisconsin Avenue Chevy Chase, MD 20815		**Copies should be sent to:** Microsoft Law and Corporate Affairs One Microsoft Way Redmond, WA 98052 USA Services Attorney (425) 936-7329 fax

TERMS AND CONDITIONS

1. Definitions. In this Agreement, a "party" or "parties" means County and/or Microsoft as the context requires. In addition, the following definitions apply:

"**Affiliate**" means (i) with regard to County, any government agency, department, office, instrumentality, division, unit or other entity of County's state or local government that is supervised by or is part of County, or which supervises County or of which County is a part, or which is under common supervision with County; together with, as mandated by law, any county, borough, commonwealth, city, municipality, town, township, special purpose district, or other similar type of governmental instrumentality located within County's state jurisdiction and geographic boundaries; provided that a state and its Affiliates shall not, for purposes of this definition, be considered to be Affiliates of the federal government and its Affiliates; and (ii) with regard to Microsoft, any legal entity that Microsoft owns, which owns Microsoft, or which is under common ownership with Microsoft. "**Ownership**" means more than 50% ownership;

"**Contractor(s)**" means any third party supplier or other provider of computer technology or related services;

"**County"** means the County of Orange, a political subdivision of the State of California, who is a party to this Agreement;

"County Data" means all data, including all text, sound, software, image or video files and any data or information within the scope of Article 7 (Data – Title to) of Attachment A, that are provided to Microsoft by, or on behalf of, County and its Affiliates in connection with Professional Services;

"**Developments**" means any computer code or materials (other than Products, Fixes or Pre-Existing Work) developed by Microsoft or in collaboration with County which is provided to County in the course of performance of a Statement of Services;

"**Fix"** or "**Fixes**" means Product fixes, modifications, enhancements, or their derivatives, that Microsoft either releases generally (such as Product service packs) or that Microsoft provides to County when performing Professional Services to address a specific issue (such as workarounds, patches, bug fixes, beta fixes and beta builds);

"**Joint Ownership**" means each party has the right to independently exercise any and all rights of ownership now known or hereinafter created or recognized, including without limitation the rights to use, reproduce, modify and distribute the Developments for any purpose, without the need for further authorization to exercise any such rights or any obligation of accounting or payment of royalties;

"Microsoft" means the Microsoft Affiliate that has entered into this Agreement and its Affiliates;

"Online Services" means the Microsoft-hosted services identified as Online Services in the Microsoft Product Terms;

"**Online Services Terms**" means the additional terms that apply to County's use of Online Services published on the Volume Licensing Site and updated from time to time;

"**Pre-Existing Work**" means any computer code or materials developed or otherwise obtained independently of the efforts of a party under a Statement of Services;

"**Product**" means all products identified in the Product Terms, such as all Software, Online Services and other web-based services, including pre-release or beta versions;

"Product Terms" means the document that provides information about Microsoft Products. The Product Terms document is published on the Volume Licensing Site and is updated from time to time;

"Professional Services" means all Product support services and Microsoft consulting services or advice provided to County under this Agreement as identified in the Attachment B, Scope of Work. "Professional Services" or "services" does not include Online Services;

"**Service Deliverables**" means any computer code or materials, other than Products or Fixes, that Microsoft leaves with County at the conclusion of Microsoft's performance of the Professional Services;

"Software" means licensed copies of Microsoft software identified on the Product Terms. Software does not include Online Services or Services Deliverables, but Software may be part of an Online Service;

"**Scope of Work**" or "Statement of Services" means any work orders, services descriptions, or other description of Professional Services identified in the Attachment B that incorporates by reference in this Agreement;

"Trade Secret" means information that is not generally known or readily ascertainable to the public, has economic value as a result, and has been subject to reasonable steps under the circumstances to maintain its secrecy;

"**use**" or "**run**" means to copy, install, use, access, display, run or otherwise interact with;

"**Use Rights**" means, with respect to any Product licensing program, the use rights or terms of service for each Product published on the Volume Licensing Site and updated from time to time. The Use Rights supersede the terms of any end user license agreement that accompanies a Product. The Use Rights for Software are published by Microsoft in the Product Terms. The Use Rights for Online Services are published in the Online Services Terms;

"**Volume Licensing Site**" means http://www.microsoft.com/licensing/contracts or a successor site.

2. Services. The precise scope of the Professional Services will be specified in a Statement of Services. Microsoft's ability to deliver the Professional Services depends upon County's full and timely cooperation, as well as the accuracy and completeness of any information County provides.

3. Use, ownership, rights and restrictions.

a. ***Products.*** Unless otherwise specified in a license agreement, use of any Product is governed by the Use Rights specific to each Product and version and by the terms of the applicable license agreement. County is responsible for paying any licensing fees associated with Products. Notice: Products will not be purchased under this Agreement.

b. ***Fixes and Services Deliverables.***

i. Fixes. Each Fix is licensed under the same terms as the Product to which it applies. If the Fix is not provided for a specific Product, any use terms Microsoft provides with the Fix will apply. If no use terms are provided, County shall have a non-exclusive, perpetual, fully paid-up license to use and reproduce the Fix solely for its internal business use. County may not modify, change the file name or combine any Fix with any non-Microsoft computer code, except as expressly permitted in a licensing agreement.

Pre-Existing Work. All rights in Pre-Existing Work will remain the sole property of the party providing the Pre-Existing Work. Each party may use, reproduce and modify the other party's Pre-Existing Work only as needed to perform obligations related to Professional Services. Upon payment in full and subject to County's compliance with this Agreement, Microsoft grants County a non-exclusive, perpetual, fully paid-up license to use, reproduce and modify (excluding object code) any Microsoft Pre-Existing Work provided as part of a Service Deliverable, solely in the form delivered to County and solely for County's internal business purposes.

ii. ***Developments.*** Upon payment in full Microsoft grants County Joint Ownership in any Developments, except as may be otherwise explicitly agreed to in a Statement of Services. County agrees to exercise its rights in Developments solely for its internal business operations only and may not otherwise resell or distribute the Developments. Each party shall be the sole owner of any modifications that it makes based upon the Developments.

iii. ***Affiliates rights.*** County may only sublicense its rights to the Services Deliverables and Sample Code granted hereunder to its Affiliates, but County's Affiliates may not sublicense these rights. County is responsible for ensuring its Affiliates' compliance with this Agreement.

c. ***Non-Microsoft software and technology.*** County is solely responsible for any non-Microsoft software or technology that County installs or uses with the Products, Fixes or Services Deliverables. County may not install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to obligations beyond those included in this Agreement.

d. ***Sample Code.*** Upon payment in full, Microsoft grants County a non-exclusive, perpetual, non-transferable license to use and modify any Software code provided by Microsoft for the purposes of illustration ("**Sample Code**") and to reproduce and distribute the object code form of the Sample Code for County's internal business purposes only and not to any unaffiliated third party.

e. ***Restrictions on use.*** County must not (and is not licensed to) (1) reverse engineer, de-compile or disassemble any Product, Fix or Service Deliverable; (2) install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to any other license terms; or (3) work around any technical limitations in a Product, Fix or Services Deliverable or restrictions in Product documentation. Except as expressly permitted in this Agreement or a Statement of Services, County must not distribute, sublicense, rent, lease or lend any Product, Fix or Service Deliverable, in whole or in part, or use them to offer hosting services to a third party.

f. ***Reservation of Rights.*** Products, Fixes, and Service Deliverables are protected by copyright and other intellectual property rights laws and international treaties. Microsoft reserves all rights not expressly granted in this Agreement. No rights will be granted or implied by waiver or estoppel.

g. ***Supportability of Products.*** Support for Products is available under the terms of a licensing agreement, a separate Statement of Services or under the terms set forth at http://support.microsoft.com or a successor site.

4. Confidentiality. Subject to the requirements of your public records and trade secret laws (if any):

"Confidential Information" is non-public information that is designated "confidential" or that a reasonable person should understand is confidential. It includes, but is not limited to, non-public information regarding either party's products, features, marketing and promotions, and the negotiated terms of this Agreement and any Statement of Services.

Confidential Information does not include information that (a) becomes publicly available without a breach of this Agreement, (b) the receiving party received from another source without a confidentiality obligation, (c) is independently developed, or (d) is a comment or suggestion volunteered about the other party's business, products or services.

Each party will take reasonable steps to protect the other's Confidential Information and will use the other party's Confidential Information only for purposes of the parties' business relationship. Neither party will disclose that Confidential Information to third parties, except to its employees, Affiliates, Contractors, advisors, and consultants ("Representatives") and then only on a need-to-know basis, under non-disclosure obligations at least as protective as this Agreement. Each party remains responsible for the use of the Confidential Information by its Representatives and, in the event of discovery of any unauthorized use or disclosure, must promptly notify the other party.

A party may disclose the other party's Confidential Information if required by law, statute, or regulation including but not limited to California Public Records Act ("CPRA"); but only after it notifies the other party (if legally permissible) to enable the other party to seek a protective order.

Neither party is required to restrict work assignments of its Representatives who have had access to Confidential Information. Each party agrees that use of information in Representatives' unaided memories in the development or deployment of the parties' respective products or services does not create liability under this Agreement or Trade Secret law, and each party agrees to limit what it discloses to the other accordingly.

These obligations apply for a period of five years after the confidential information is received.

5. Compliance with applicable laws, privacy and security.

a. County consents to processing personal information by Microsoft and its agents to facilitate the subject matter of this Agreement. County will obtain all required consents from third parties (including County's contacts, resellers, distributors, administrators, and employees) under applicable privacy and data protection law before providing personal information to Microsoft.

b. Personal information collected through Professional Services (i) may be transferred, stored and processed in the United States and (ii) will be subject to the privacy terms specified in the Use Rights. Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention and processing of personal data from the European Economic Area and Switzerland.

c. **U.S. Export.** Microsoft Products, Fixes and Services Deliverables are subject to U.S. export jurisdiction. County must comply with all applicable international and national laws, including the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, and end-user, end use and destination restrictions by U.S. and other governments related to Microsoft Products, services, and technologies.

6. Warranties.

a. ***Limited warranties and remedies – Professional Services.*** Microsoft warrants that it will perform Professional Services with professional care and skill. If Microsoft fails to do so, and County notifies Microsoft within 90 days of date of the Professional Services were performed, then Microsoft will, at its discretion, either re-perform the Professional Services or return the price paid for them. These remedies are County's sole remedies for breach of warranties in this section. County waives any breach of warranty claims not made during the warranty period.

b. ***Exclusions.*** The warranties in this section do not cover problems caused by accident, abuse or use in a manner inconsistent with this Agreement, including failure to meet minimum system requirements. These warranties do not apply to free, trial, pre-release or beta Products or to components of Products that County is permitted to redistribute. ***DISCLAIMER.*** **Except for the limited warranties above, Microsoft provides no other warranties or conditions and disclaims any other express, implied or statutory warranties, including warranties of merchantability, fitness for a particular purpose, title and non-infringement.**

7. Defense of third party claims.

The parties will defend each other against the third-party claims described in this section and will pay the amount of any resulting adverse final judgment or approved settlement, but only if the defending party is promptly notified in writing of the claim and has the right to control the defense and any settlement of it. The party being defended must provide the defending party with all requested assistance, information and authority. The defending party will reimburse the other party for reasonable out-of-pocket expenses it incurs in providing assistance. This section describes the parties' sole remedies and entire liability for such claims.

- ***a. By Microsoft.*** Microsoft will defend County against any third-party claim to the extent it alleges that any Fix or Services Deliverable made available by Microsoft for a fee and used within the scope of Section 3 of this Agreement (unmodified from the form provided by Microsoft and not combined with anything else) violates the law or damages a third party or misappropriates a trade secret or directly infringes a patent, copyright, or trademark or other proprietary right of a third party. If Microsoft is unable to resolve a claim of infringement under commercially reasonable terms, it may, at its option, either (1) modify or replace the Fix or Services Deliverable with a functional equivalent; or (2) terminate County's intellectual property rights and refund any fees paid for such Services Deliverable(s). Microsoft will not be liable for any claims or damages due to County's continued use of a Product, Fix or Services Deliverable after being notified to stop due to a third party claim.

- **b.** ***By County.*** To the extent permitted by applicable law, County will defend Microsoft against any third-party claim to the extent it alleges that County's use of any Fix or Services Deliverable alone or in combination with anything else, violates the law or damages a third party.

8. Limitations of liability.

Each party's maximum, aggregate liability to the other is limited to direct damages finally awarded in an amount not to exceed the amounts County was required to pay for the applicable Statement of Services during the term of the Statement of Services, subject to the following.

- ***a. Free Professional Services and Distributable Code.*** For Professional Services provided free of charge and code that County is authorized to redistribute to third parties without a separate payment to Microsoft, Microsoft's liability is limited to direct damages finally awarded up to US$5000.

- ***b. Exclusions.*** **In no event will either party be liable for any indirect, incidental, special, punitive, or consequential damages, or for loss of use, loss of business information, loss of revenue or interruption of business, however caused or on any theory of liability.**

- ***c. Exceptions.*** No limitation or exclusions will apply to liability arising out of either party's (1) confidentiality obligations (except for all liability related to County Data, which will remain subject to the limitations and exclusions above); (2) defense obligations; or (3) violation of the other party's intellectual property rights.

9. Miscellaneous.

- ***a. Survival.*** All provisions survive termination or expiration of this Agreement, except those requiring performance only during the term of a Statement of Services.

- ***b. Agreement not exclusive.*** County is free to enter into agreements to license, use or promote non-Microsoft products or services.

- ***c. Use of Contractors.*** Microsoft may use Contractors to perform Professional Services, but will be responsible for their performance subject to the terms of this Agreement.

- ***d. No transfer of ownership.*** Microsoft does not transfer ownership rights in any Product. The Products are protected by copyright and other intellectual property rights, laws and international treaties.

e. ***Calendar days.*** Any reference in this Agreement to "day" will be a calendar day, except references that specify "business day."

f. ***Cost or pricing data*****.** We will not, under any circumstances, accept any statement of services that would require the submission of cost or pricing data.

g. **No third-party beneficiaries.** This Agreement does not create any third-party beneficiary rights.

h. **Order of Precedence.** This Agreement consist of this Agreement and Attachments A—G. All terms and provisions set forth in Attachments A—G are hereby incorporated by reference with the same force and effect as though fully set forth herein. This Agreements including its Attachments A—G, shall be read to be consistent and complementary. In the event of any inconsistency between the articles, attachments, or provisions which constitute this Agreement, the following order of precedence shall apply:

1. The terms and provisions in the body of this Agreement
2. Attachment A: County Terms and Conditions
3. Attachment B: Scope of Work
4. Attachment C: Compensation and Payment
5. Attachment D: Microsoft Business Associate Agreement
6. Attachment E: Cyber Security Best Practices Manual
7. Attachment F: Information Technology Usage
8. Attachment G: IT Security Policy 2009

ATTACHMENT A
COUNTY TERMS AND CONDITIONS

General Terms and Conditions:

A. **Governing Law and Venue**: This Agreement has been negotiated and executed in the state of California and shall be governed by and construed under the laws of the state of California. In the event of any legal action to enforce or interpret this Agreement, the sole and exclusive venue shall be a court of competent jurisdiction located in Orange County, California, and the parties hereto agree to and do hereby submit to the jurisdiction of such court, notwithstanding Code of Civil Procedure Section 394. Furthermore, the parties specifically agree to waive any and all rights to request that an action be transferred for trial to another County.

B. **Entire Agreement**: This Agreement contains the entire Agreement between the parties with respect to the matters herein, and there are no restrictions, promises, warranties or undertakings other than those set forth herein or referred to herein. No exceptions, alternatives, substitutes or revisions are valid or binding on County unless authorized by County in writing. Electronic acceptance of any additional terms, conditions or supplemental contracts by any County employee or agent, including but not limited to installers of software, shall not be valid or binding on County unless accepted in writing by County's Procurement Officer or designee.

C. **Amendments**: No alteration or variation of the terms of this Agreement shall be valid unless made in writing and signed by the parties; no oral understanding or agreement not incorporated herein shall be binding on either of the parties; and no exceptions, alternatives, substitutes or revisions are valid or binding on County unless authorized by County in writing.

D. **Taxes**: Unless otherwise provided herein or by law, price quoted does not include California state sales or use tax. Microsoft shall indicate California Board of Equalization permit number and sales permit number on invoices, if California sales tax is added and collectable. If no permit numbers are shown, sales tax will be deducted from payment. The Auditor-Controller will then pay use tax directly to the State of California in lieu of payment of sales tax to the Microsoft.

E. **Acceptance/Payment**: Unless otherwise agreed to in writing by County, 1) acceptance shall not be deemed complete unless in writing and until all the goods/services have actually been received, inspected, and 2) payment shall be made in arrears after satisfactory acceptance.

F. **Patent/Copyright Materials/Proprietary Infringement**: Unless otherwise expressly provided in this Agreement, Microsoft shall be solely responsible for clearing the right to use any patented or copyrighted materials in the performance of this Agreement. Microsoft warrants that any software as modified through services provided hereunder will not infringe upon or violate any patent, proprietary right, or trade secret right of any third party.

G. **Assignment**: The terms, covenants, and conditions contained herein shall apply to and bind the heirs, successors, executors, administrators and assigns of the parties. Furthermore, neither the performance of this Agreement nor any portion thereof may be assigned by Microsoft without the express written consent of County. Any attempt by Microsoft to assign the performance or any portion thereof of this Agreement without the express written consent of County shall be invalid and shall constitute a breach of this Agreement.

H. **Non-Discrimination**: In the performance of this Agreement, Microsoft agrees that it will comply with the requirements of Section 1735 of the California Labor Code and not engage nor permit any subcontractors to engage in discrimination in employment of persons because of the race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, or sex of such persons. Microsoft acknowledges that a violation of this provision shall subject Microsoft to penalties pursuant to Section 1741 of the California Labor Code.

I. **Termination**: In addition to any other remedies or rights it may have by law, County has the right to immediately terminate this Agreement without penalty for cause or after 30 days' written notice without cause, unless otherwise specified. Cause shall be defined as any material breach of contract, any material misrepresentation or fraud on the part of Microsoft.

J. **Consent to Breach Not Waiver**: No term or provision of this Agreement shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented. Any consent by any party to, or waiver of, a breach by the other, whether express or implied, shall not constitute consent to, waiver of, or excuse for any other different or subsequent breach.

K. **Independent Contractor**: Microsoft shall be considered an independent contractor and neither Microsoft, its employees, nor anyone working under Microsoft shall be considered an agent or an employee of County. Neither Microsoft, its employees nor anyone working under Microsoft shall qualify for workers' compensation or other fringe benefits of any kind through County.

L. **Changes**: Microsoft shall make no changes in the work or perform any additional work without the County's specific written approval.

M. **Change of Ownership/Name, Litigation Status, Conflict of Interest Status**: Microsoft agrees that if there is a change or transfer in ownership of Microsoft's business prior to completion of this Agreement, and the County agrees to an assignment of the Agreement, the new owners shall be required under the terms of sale or other instruments of transfer to assume Microsoft's duties and obligations contained in this Agreement and complete them to the satisfaction of the County.

County reserves the right to immediately terminate the Agreement in the event the County determines that the assignee is not qualified or is otherwise unacceptable to the County for the provision of services under the Agreement.

In addition, Microsoft has the duty to notify the County in writing of any change in Microsoft's status with respect to name changes that do not require an assignment of the Agreement. Microsoft is also obligated to notify the County in writing if Microsoft becomes a party to any litigation against the County, or a party to litigation that may reasonably affect Microsoft's performance under the Agreement, as well as any potential conflicts of interest between Microsoft and County that may arise prior to or during the period of Agreement performance. While Microsoft will be required to provide this information without prompting from the County any time there is a change in Microsoft's name, conflict of interest or litigation status, Microsoft must also provide an update to the County of its status in these areas whenever requested by the County.

Microsoft shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with County interests. In addition to Microsoft, this obligation shall apply to Microsoft's employees, agents, and subcontractors associated with the provision of goods and services provided under this Agreement. Microsoft's efforts shall include, but not be limited to establishing rules and procedures preventing its employees, agents, and subcontractors from providing or offering gifts, entertainment, payments, loans or other considerations which could be deemed to influence or appear to influence County staff or elected officers in the performance of their duties.

N. **Force Majeure**: Microsoft shall not be assessed with liquidated damages or unsatisfactory performance penalties during any delay beyond the time named for the performance of this Agreement caused by any act of God, war, civil disorder, employment strike or other cause beyond its reasonable control, provided Microsoft gives written notice of the cause of the delay to County within thirty-six (36) hours of the start of the delay and Microsoft avails itself of any available remedies.

O. **Confidentiality**: Microsoft agrees to maintain the confidentiality of all County and County-related records and information pursuant to all statutory laws relating to privacy and confidentiality that currently exist or exist at any time during the term of this Agreement. All such records and information shall be considered confidential and kept confidential by Microsoft and Microsoft's staff, agents and employees.

P. **Compliance with Laws**: Microsoft represents and warrants that services to be provided under this Agreement shall fully comply, at Microsoft's expense, with all applicable standards, laws, statutes, restrictions, ordinances, requirements, and regulations (collectively "laws"), including, but not limited to those issued by County in its governmental capacity and all other laws applicable to the services at the time services are provided to and accepted by County.

Q. **Severability**: If any term, covenant, condition, or provision of this Agreement is held by a court of competent jurisdiction to be invalid, void or unenforceable, the remainder of the provisions hereof shall remain in full force and effect and shall in no way be affected, impaired or invalidated thereby.

R. **Attorney Fees**: In any action or proceeding to enforce or interpret any provision of this Agreement, or where any provision hereof is validly asserted as a defense, each party shall bear its own attorney's fees, costs and expenses.

S. **Interpretation**: This Agreement has been negotiated at arm's length and between persons sophisticated and knowledgeable in the matters dealt with in this Agreement. In addition, each party has been represented by experienced and knowledgeable independent legal counsel of its own choosing or has knowingly declined to seek such counsel despite being encouraged and given the opportunity to do so. Each party further acknowledges that it has not been influenced to any extent whatsoever in executing this Agreement by any other party hereto or by any person representing them, or both. Accordingly, any rule or law (including California Civil Code Section 1654) or legal decision that would require interpretation of any ambiguities in this Agreement against the party that has drafted it is not applicable and is waived. The provisions of this Agreement shall be interpreted in a reasonable manner to affect the purpose of the parties and this Agreement.

T. **Employee Eligibility Verification**: Microsoft warrants that it fully complies with all Federal and State statutes and regulations regarding the employment of aliens and others and that all its employees performing work under this Agreement meet the citizenship or alien status requirement set forth in Federal statutes and regulations. Microsoft shall obtain, from all employees, consultants and subcontractors performing work hereunder, all verification and other documentation of employment eligibility status required by Federal or State statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986, 8 U.S.C. §1324 et seq., as they currently exist and as they may be hereafter amended. Microsoft shall retain all such documentation for all covered employee, consultants and subcontractors for the period prescribed by the law. Microsoft shall indemnify, defend with counsel approved in writing by County, and hold harmless, the County, its agents, officers, and employees from employer sanctions and any other liability which may be assessed against Microsoft actor or the County or both in connection with any alleged violation of any Federal or State statutes or regulations pertaining to the eligibility for employment of any persons performing work under this Agreement.

U. **Audits/Inspection**: Microsoft shall keep and make available for the inspection and audit of or by the County or its authorized employees, agents or representatives during normal business hours, at the County's cost, all data, materials and information relating specifically to Microsoft's performance under this Agreement. Any such inspection and/or audit will be confined to those matters connected with the performance of the Agreement including, but not limited to, the costs of administering the Agreement. The County will provide reasonable notice of such an audit or inspection and such date will be mutually agreed upon.

Microsoft agrees to maintain such records for possible audit for a minimum of three years after final payment, unless a longer period of records retention is stipulated under this Agreement or by law. Microsoft agrees to allow interviews of any employees or others who might reasonably have information related to such records. Further, Microsoft agrees to include a similar right to the County to audit records related to performance of this Agreement.

Should Microsoft cease to exist as a legal entity, Microsoft's records pertaining to this agreement shall be forwarded to the surviving entity in a merger or acquisition or, in the event of liquidation, to the County's project manager.

V. **Contingency of Funds**: Microsoft acknowledges that funding or portions of funding for this Agreement may be contingent upon state budget approval; receipt of funds from, and/or obligation of funds by, the State of California to County; and inclusion of sufficient funding for the services hereunder in the budget approved by County's Board of Supervisors for each fiscal year covered by this Agreement. If such approval, funding or appropriations are not forthcoming, or are otherwise limited, County may immediately terminate or modify this Agreement without penalty.

W. **Expenditure Limit**: Microsoft shall notify the County of Orange assigned Deputy Purchasing Agent in writing when the expenditures against the Agreement reach 75 percent of the dollar limit on the Agreement. The County will not be responsible for any expenditure overruns and will not pay for work exceeding the dollar limit on the Agreement unless a change order to cover those costs has been issued.

Additional Terms and Conditions:

1. **Scope of Agreement**: This Agreement specifies the contractual terms and conditions by which the County will procure Microsoft Identity Manager Implementation Services from Microsoft Corporation as further detailed in the Scope of Work, identified and incorporated herein by this reference as "Attachment A".

2. **Adjustments – Scope of Work**: No adjustments made to the Scope of Work will be authorized without the prior written approval of the County assigned Deputy Purchasing Agent.

3. **Term of Agreement**: This Agreement shall commence upon execution of all necessary signatures effective May 15, 2019 through and including May 14, 2021. The County does not have to give reason if it elects not to renew.

4. **Breach of Agreement**: The failure of Microsoft to comply with any of the provisions, covenants or conditions of this Agreement shall be a material breach of this Agreement. In such event the County may, and in addition to any other remedies available at law, in equity, or otherwise specified in this Agreement:

i. Terminate the Agreement immediately, pursuant to Article I herein;

ii. Afford Microsoft written notice of the breach and ten calendar days or such shorter time that may be specified in this Agreement within which to cure the breach;

iii. Discontinue payment to Microsoft for and during the period in which Microsoft is in breach; and

iv. Offset against any monies billed by Microsoft but yet unpaid by the County those monies disallowed pursuant to the above.

5. **Conflict of Interest – Microsoft's Personnel**: Microsoft shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with the best interests of the County. This obligation shall apply to Microsoft; Microsoft's employees, agents, and subcontractors associated with accomplishing work and services hereunder. Microsoft's efforts shall include, but not be limited to establishing precautions to prevent its employees, agents, and subcontractors from providing or offering gifts, entertainment, payments, loans or other considerations which could be deemed to influence or appear to influence County staff or elected officers from acting in the best interests of the County.

6. **County of Orange Child Support**: Microsoft certifies it is in full compliance with all applicable federal and state reporting requirements regarding its employees and with all lawfully served Wage and Earnings Assignment Orders and Notices of Assignments and will continue to be in compliance throughout the term of the Agreement with the County of Orange. Failure to comply shall constitute a material breach of the Agreement and failure to cure such breach within 60 calendar days of notice from the County shall constitute grounds for termination of the Agreement.

7. **Data – Title to**: All materials, documents, data or information obtained from the County data files or any County medium furnished to Microsoft in the performance of this Agreement will at all times remain the property of the County. Such data or information may not be used or copied for direct or indirect use by Microsoft after completion or termination of this Agreement without the express written consent of the County. All materials, documents, data or information, including copies, must be returned to the County at the end of this Agreement.

8. **Microsoft Personnel – Reference Checks**: Microsoft warrants that all persons employed to provide service under this Agreement have satisfactory past work records indicating their ability to adequately perform the work under this Agreement. Microsoft's employees assigned to this project must meet character standards as demonstrated by background investigation and reference checks, coordinated by the agency/department issuing this Agreement.

9. **Microsoft's Expense**: Microsoft will be responsible for all costs related to photo copying, telephone communications, fax communications, and parking while on County sites during the performance of work and services under this Agreement.

10. **Microsoft's Project Manager and Key Personnel**: Microsoft shall appoint a Project Manager to direct Microsoft's efforts in fulfilling Microsoft's obligations under this Agreement. This Project Manager shall be subject to approval by the County and shall not be changed without the written consent of the County's Project Manager, which consent shall not be unreasonably withheld.

    Microsoft's Project Manager shall be assigned to this project for the duration of the Agreement and shall diligently pursue all work and services to meet the project time lines. The County's Project Manager shall have the right to require the removal and replacement of Microsoft's Project Manager from providing services to the County under this Agreement. The County's Project manager shall notify Microsoft in writing of such action. Microsoft shall accomplish the removal within five (5) business days after written notice by the County's Project Manager. The County's Project Manager shall review and approve the appointment of the replacement for Microsoft's Project Manager. The County is not required to provide any additional information, reason or rationale in the event it requires the removal of Microsoft's Project Manager from providing further services under the Agreement.

11. **Equal Employment Opportunity**: Microsoft shall comply with U.S. Executive Order 11246 entitled, "Equal Employment Opportunity" as amended by Executive Order 11375 and as supplemented in Department of Labor regulations (41 CFR, Part 60) and applicable State of California regulations as may now exist or be amended in the future. Microsoft shall not

discriminate against any employee or applicant for employment on the basis of race, color, national origin, ancestry, religion, sex, marital status, political affiliation or physical or mental condition.

Regarding handicapped persons, Microsoft will not discriminate against any employee or applicant for employment because of physical or mental handicap in regard to any position for which the employee or applicant for employment is qualified. Microsoft agrees to provide equal opportunity to handicapped persons in employment or in advancement in employment or otherwise treat qualified handicapped individuals without discrimination based upon their physical or mental handicaps in all employment practices such as the following: employment, upgrading, promotions, transfers, recruitments, advertising, layoffs, terminations, rate of pay or other forms of compensation, and selection for training, including apprenticeship. Microsoft agrees to comply with the provisions of Sections 503 and 504 of the Rehabilitation Act of 1973, as amended, pertaining to prohibition of discrimination against qualified handicapped persons in all programs and/or activities as detailed in regulations signed by the Secretary of the Department of Health and Human Services effective June 3, 1977, and found in the Federal Register, Volume 42, No. 68 dated May 4, 1977, as may now exist or be amended in the future.

Regarding Americans with disabilities, Microsoft agrees to comply with applicable provisions of Title 1 of the Americans with Disabilities Act enacted in 1990 as may now exist or be amended in the future.

12. **Civil Rights**: Microsoft attests that services provided shall be in accordance with the provisions of Title VI and Title VII of the Civil Rights Act of 1964, as amended, Section 504 of the Rehabilitation Act of 1973, as amended; the Age Discrimination Act of 1975 as amended; Title II of the Americans with Disabilities Act of 1990, and other applicable State and federal laws and regulations prohibiting discrimination on the basis of race, color, national origin, ethnic group identification, age, religion, marital status, sex or disability.

13. **Compliance with County Information Technology Policies and Procedures**:

Policies and Procedures

Microsoft, Microsoft subcontractors, Microsoft personnel, and all other agents and representatives of Microsoft, will at all times comply with and adhere by all Information Technology (IT) policies and procedures of the County that are provided or made available to Microsoft that reasonably pertain to Microsoft (and of which Microsoft has been provided with advance notice) in connection with Microsoft's performance under this Agreement including, but not limited to requirements as set forth in Attachments E-G. Microsoft shall cooperate with the County in ensuring Microsoft's compliance with the IT policies and procedures described in this Agreement and as adopted by the County from time-to-time, and any material violations or disregard of such IT policies or procedures shall, in addition to all other available rights and remedies of the County, be cause for termination of this Agreement. In addition to the foregoing, Microsoft shall comply with the following:

Security and Policies

All performance under this Agreement, shall be in accordance with the County's security requirements, policies, and procedures as set forth above and as modified, supplemented, or replaced by the County from time to time, in its sole discretion, by providing Microsoft with a written copy of such revised requirements, policies, or procedures reasonably in advance of the date that they are to be implemented and effective (collectively, the "Security Policies"). Microsoft shall at all times use industry best practices and methods with regard to the prevention, detection, and elimination, by all appropriate means, of fraud, abuse, and other inappropriate or unauthorized access to County systems accessed in the performance of services in this Agreement.

Information Access

The County may require all Microsoft personnel performing services under this Agreement to execute a confidentiality and non-disclosure Agreement concerning access protection and data security in the form provided by County. The County shall authorize, and Microsoft shall issue, any necessary information-access mechanisms, including access IDs and passwords, and in no event shall Microsoft permit any such mechanisms to be shared or used by other than the individual Microsoft personnel to whom issued. Microsoft shall provide each Microsoft Person with only such level of access as is required for such individual to perform his or her assigned tasks and functions. All County systems, and all data and software contained therein, including County data, County hardware and County software, used or accessed by Microsoft: (a) shall be used and accessed by Microsoft solely and exclusively in the performance of their assigned duties in connection with, and in furtherance of, the performance of Microsoft's obligations hereunder; and (b) shall not be used or accessed except as expressly permitted hereunder, or commercially exploited in any manner whatsoever, by Microsoft, at any time.

Enhanced Security Procedures

The County may, in its discretion, designate certain areas, facilities, or systems as requiring a higher level of security and access control. The County shall notify Microsoft in writing reasonably in advance of any such designation becoming effective. Any such notice shall set forth in reasonable detail the enhanced security or access-control procedures, measures, or requirements that Microsoft shall be required to implement and enforce, as well as the date on which such procedures and measures shall take effect. Microsoft shall fully comply with and abide by all such enhanced security and access measures and procedures as of such date.

Breach of Security

Any breach or violation by Microsoft of any of the foregoing shall be deemed a material breach of a material obligation of Microsoft under this Agreement and may be deemed an incurable and material breach of a material obligation of Microsoft under this Agreement resulting in termination.

14. **Security Breach Notification**: In the event Microsoft becomes aware that it is the proximate cause of any act, error or omission, negligence, misconduct, or security incident including unsecure or improper data disposal, theft, loss, unauthorized use and disclosure or access, that compromises or is suspected to compromise the security, confidentiality, or integrity of County Data or the physical, technical, administrative, or organizational safeguards put in place Microsoft that relate to the security, confidentiality, or integrity of County Data, Microsoft shall, at its own expense, (1) immediately notify the County's Chief Information Security Officer and County Privacy Officer of such occurrence and perform a root cause analysis thereon, (2) investigate such occurrence, (3) provide a remediation plan, acceptable to County, to address the occurrence and prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event, and (5) cooperate with County and any law enforcement or regulatory officials investigating such occurrence, including but not limited to making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by County and/or any law enforcement or regulatory officials, and (6) perform or take any other actions required to comply with applicable law as a result of the occurrence (at the direction of County). County shall make the final decision on notifying County persons, entities, employees, service providers, and/or the general public of such occurrence, and the implementation of the remediation plan. If notification to particular persons is required under any law or pursuant to any of County's privacy or security policies, then notifications to all persons and entities who are affected by the same event shall be considered legally required. Microsoft shall reimburse County for all notification related costs incurred by County arising out of or in connection with any such occurrence due to Microsoft's acts, errors or omissions, negligence, and/or misconduct resulting in a requirement for legally required notifications.

In the case of personally identifiable information, Microsoft shall provide third-party credit and identity monitoring services to each of the affected individuals for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than twelve (12) months following the date of notification to such individuals.

Microsoft shall indemnify, defend and hold County and County Indemnitees harmless from and against any and all claims, including reasonable attorneys fees, costs, and expenses incidental thereto, which may be suffered by, accrued against, charged to, or recoverable from County in connection with the occurrence.

15. Disputes – Agreement:

A. The parties shall deal in good faith and attempt to resolve potential disputes informally. If the dispute concerns a question of fact arising under the terms of this Agreement and is not disposed of in a reasonable period of time by Microsoft's Project Manager and the County's Project Manager, such matter shall be brought to the attention of the other party by way of the following process:

1. The party shall submit to the agency/department assigned authority of the other party a written demand for a final decision regarding the disposition of any dispute between the parties arising under, related to, or involving this Agreement.

2. The party's written demand shall be fully supported by factual information, and, if such demand involves a cost adjustment to the Agreement, the party shall include with the demand a written statement signed by a senior official indicating that the demand is made in good faith, that the supporting data are accurate and complete, and that the amount requested accurately reflects the Agreement adjustment for which the party believes the opposing party is liable.

B. Pending the final resolution of any dispute arising under, related to, or involving this Agreement, Microsoft agrees to diligently proceed with the performance of this Agreement, including the delivery of goods and/or provision of Services. Microsoft's failure to diligently proceed shall be considered a material breach of this Agreement.

Any final decision shall be expressly identified as such, shall be in writing, and shall be signed by the County Deputy Purchasing Agent or his designee and Microsoft's appointed authority. If a party fails to render a decision within 90 days after receipt of the original written demand, it shall be deemed a final decision adverse to the opposing party's contentions. Nothing in this section shall be construed as affecting the either party's right to terminate the Agreement for cause or termination for convenience as stated in Article I herein.

16. Errors and Omissions: All reports, files and other documents prepared and submitted by Microsoft shall be complete and shall be carefully checked by the professional(s) identified by Microsoft as project manager and key personnel attached hereto, prior to submission to the County. Microsoft agrees that County review is discretionary and Microsoft shall not assume that the County will discover errors and/or omissions. If the County discovers any errors or omissions prior to approving Microsoft's reports, files and other written documents, the reports, files or documents will be returned to Microsoft for correction. Should the County or others discover errors or omissions in the reports, files or other written documents submitted by Microsoft after County approval thereof, County approval of Microsoft's reports, files or documents shall not be used as a defense by Microsoft in any action between the County and Microsoft, and the reports, files or documents will be returned to Microsoft for correction.

17. **Gratuities**: Microsoft warrants that no gratuities, in the form of entertainment, gifts or otherwise, were offered or given by Microsoft or any agent or representative of Microsoft to any officer or employee of the County with a view toward securing the Agreement or securing favorable treatment with respect to any determinations concerning the performance of the Agreement. For breach or violation of this warranty, the County shall have the right to terminate the Agreement, either in whole or in part, and any loss or damage sustained by the County in procuring on the open market any goods or services which Microsoft agreed to supply shall be borne and paid for by Microsoft. The rights and remedies of the County provided in the clause shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Agreement.

18. **Microsoft's Records**: Microsoft shall keep true and accurate accounts, records, books and data which shall correctly reflect the business transacted by Microsoft in accordance with generally accepted accounting principles

19. **Non-Appropriation Clause**: This Agreement is subject to and contingent upon applicable budgetary appropriations being approved by the County of Orange Board of Supervisors for each fiscal year during the term of this contract. If such appropriations are not approved, the contract will be terminated without penalty to the County.

20. **Security of County Data**: Microsoft represents and warrants that Microsoft's personnel who have access to County data meet the necessary background checks, as conveyed to Microsoft, and will adhere to County's confidentiality requirements as set forth in this Agreement. Microsoft's personnel shall not view any human readable data unless authorized in writing by County. All security incidents involving Microsoft personnel or Microsoft's subcontractors, including unsecure or improper data disposal, theft, loss, unauthorized disclosure, incorrect transmission of data, hacking, IT Incident, and unauthorized Use/Access associated with County data, must be promptly reported to the County Cyber Security contacts:

Linda Le, CHPC, CHC, CHP
County Privacy Officer
1055 N. Main Street, 6th Floor
Santa Ana, CA 92701
Office: (714) 834-4082
Email: linda.le@ceoit.ocgov.com
privacyofficerinbox@ceoit.ocgov.com
securityadmin@ceoit.ocgov.com

21. **Termination – Orderly**: After receipt of a termination notice from the County, Microsoft may submit to the County a termination claim, if applicable. Such claim shall be submitted promptly, but in no event later than 60 days from the effective date of the termination, unless one or more extensions in writing are granted by the County upon written request of Microsoft. Upon termination County agrees to pay Microsoft for all Services performed prior to termination which meet the requirements of the Agreement, provided, however, that such compensation combined with previously paid compensation shall not exceed the total compensation set forth in the Agreement. Upon termination or other expiration of this Agreement, each party shall promptly return to the other party all papers, materials, and other properties of the other held by each for purposes of performance of the Agreement.

22. **Usage**: No guarantee is given by the County to Microsoft regarding usage of this Agreement. Usage figures, if provided, are approximations. Microsoft agrees to supply services and/or commodities requested, as needed by the County of Orange, at rates/prices listed in the Agreement, regardless of quantity requested.

23. **Waivers – Agreement**: The failure of the County in any one or more instances to insist upon strict performance of any of the terms of this Agreement or to exercise any option contained herein shall not be construed as a waiver or relinquishment to any extent of the right to assert or rely upon any such terms or option on any future occasion.

24. **Notices**: Any and all notices permitted or required to be given hereunder shall be deemed duly given (1) upon actual delivery, if delivery is by hand, (2) upon delivery by the United States mail if delivery is by postage paid registered or certified return receipt requested mail, or (3) upon delivery via electronic mail with confirmation receipt. Each such notice shall be sent to the respective party at the address indicated below or to any other address as the respective parties may designate from time to time.

Microsoft:
Microsoft Corporation
Attn: David Gallagher
Director of Contracts
12012 Sunset Hills Road
Reston, VA 20190
Phone: 703-673-7871
Email: dgallagh@microsoft.com

For County:
Department:
County of Orange/OCIT
Attn: Mai Le
1055 N. Main Street, 6th Floor,
Santa Ana, CA 92701
Phone: 714-834-7213
Email: mai.le@ocit.ocgov.com

Contracts & Purchasing:
County of Orange/OCIT Purchasing
Attn: Annie Pham, DPA
1055 N. Main Street, 6nd Floor
Santa Ana, CA 92701
Email: annie.pham@ocit.ocgov.com

SIGNATURE PAGE

In WITNESS WHEREOF, the parties hereto have executed this Agreement on the dates shown opposite their respective signatures below:

MICROSOFT CORPORATION*

DATE: 4/15/2019

SIGNATURE: DocuSigned by: David T. Gallagher C5E4EEEE6A2E45D

PRINT NAME: David T. Gallagher

TITLE: Director of Contracts

DATE: ______________

SIGNATURE: ______________________________

PRINT NAME: ______________________________

TITLE: ______________________________

** The first corporate officer signature must be one of the following: 1) the Chairman of the Board; 2) the President; 3) any Vice President. The second corporate officer signature must be one of the following: 1) Secretary; 2) Assistant Secretary; 3) Chief Financial Officer; 4) Assistant Treasurer.*

In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution demonstrating the legal authority of the signature to bind the company.

COUNTY OF ORANGE

A political subdivision of the State of California

DATE: 5/9/19

SIGNATURE: Annie Pham

PRINT NAME: ANNIE PHAM

TITLE: Deputy Purchasing Agent – PCS

APPROVED AS TO FORM, County Counsel, County of Orange, California

Daniel Shepherd — Deputy County Counsel

Print Name — Title

Signature — Date 4.16.19

ATTACHMENT B
SCOPE OF WORK

1. Project Objectives and Scope

1.1 Objectives

The purpose of this project is to design and implement an identity and access management solution for Orange County based on Microsoft Identity Manager (MIM) 2016. This solution will facilitate the management of user, contact and group objects in 27 Active Directory (AD) domains contained in 18 AD forests as well as the OCProfile SQL database from the MIM Portal. It will also help automate the management of user accounts and associated entitlements based on the data imported from the HR system.

This project will also perform a synchronization of mail contacts between 18 Microsoft Exchange organizations which are associated with the 18 in-scope AD forests.

1.2 Areas within Scope

1.2.1 General Project Scope

Microsoft will provide services in support of the following scope.

Table 1: Services in Scope

Service, Feature or Function	Description	Key Scope Assumptions
Conduct Envisioning and Assessment workshops	• Assess the current environment to understand how identities are managed today • Collect County requirements • Assess the 27 in-scope Active Directory domains and their synchronization of identity data to the OC-Global domain, OCID-GLOBAL domain and the OCProfile database	County stakeholders and subject matter experts (SMEs) will participate in workshops.
Global Address List Synchronization	• Assess the current Orange County messaging environment to understand which portions of that environment will be in scope	GAL Synchronization will only include the 18 in-scope AD forests and MS Exchange organizations.
Access controls	Design and implement access controls for each persona who will be interacting with the portal. Personas include: • Regular users • Service desk • Account administrators • Distribution group administrators • Security group administrators	The number of personas will be limited to 5.
Schema and user interface customizations	• Design and implement the extensions to the MIM schema, including additional attributes per the County requirements	The number of new attributes added to the schema and to the web forms will be limited to 20.

	• Design and implement the placement of these attributes in the web forms used to manage users and groups from the MIM Portal	
Configure the applicable Database Connector for connectivity to the HR System	• Design data Import from HR, including delta change detection • Design data Export to HR • Install and Configure the Generic SQL Connector	Orange County will be responsible for setting up the views, tables, triggers or stored procedures needed by MIM to read and write to the HR database through this connector.
Synchronize user information between AD and HR	• Design and Implement synchronization rules to: o Join the user records imported from HR with the ones imported from AD o Synchronize select attributes from HR to AD o Synchronize select attributes from AD to HR	
User management in AD from HR (Employees)	Design and implement workflows to provision and deprovision user accounts in AD based on the user profile information imported from HR. Workflows include: • Unique account name and random strong password generation • Construction of the DisplayName • Creation of the user account in the right domain and AD organizational unit based on an employee HR attribute • Notification sent to the manager and Service Desk on successful account creation • On termination from HR, disable the account and move it to the disabled organization unit followed by deletion 90 days later • Upon re-activation, re-enable the user account and move it back to the correct organization unit; if the user account has been deleted, re-create the user account in AD	Employee user attributes will be built based on other attributes imported into the MIM service database. The number of user attributes built or validated is limited to 20. County will be responsible for providing an HR attribute to AD domain mapping to control to which of the agency domains a user account will be created.
User management in AD from MIM Portal (Contractors)	Design and implement workflows to provision and deprovision Contractor user	Contractor user attributes will be built based on other attributes entered the MIM

	accounts in AD based on the user profile information imported from the MIM Portal. Workflows include: • Unique account name and random strong password generation • Construction of the DisplayName • Creation of the user account in the right domain and AD organizational unit based on a Contractor department attribute set in the MIM Portal • Notification sent to the manager and Service Desk on successful account creation • On termination in the MIM Portal, disable the account and move it to the disabled organization unit followed by deletion 90 days later • Upon re-activation in the MIM Portal, re-enable the user account and move it back to the correct organization unit; if the user account has been deleted, re-create the user account in AD	portal through end-user data entry. The number of Contractor user attributes built or validated is limited to 20.
User Transfer between departments in different domains	When a user transfers from one department to another and this transfer results in a change of user domain, the following actions will occur: • Actions will occur when the department value is received from HR for employees or from the MIM portal for Microsoft • When the user department value changes, o Disable the account current domain and move it to the disabled organization unit followed by deletion 90 days later o Provision a new account in the new domain corresponding to the new department value • Notification sent to the new manager and Service Desk of user transfer	Mail attributes will not be transitioned to the new user. Mailbox management is out of scope. User group memberships will not be preserved. The transfer process results in a new user object whose entitlements must be granted after creation.
Entitlement Management in	• Design and implement workflows to request the provisioning/de-provisioning of user accounts and associated entitlements for up to 5	

loosely connected systems	different systems without using MIM connectors • Based on the user data imported from HR for a new hire, or the entitlement selected for an existing user from the MIM Portal, the following workflows take place: o Email notification is sent to an approver to request for approval of the access requested, o Upon approval, an email notification is sent to the system administrator to request manual provisioning of the user account and associated entitlements • When the user is terminated in HR or from the MIM Portal an email notification is sent to all system administrators to request the deprovisioning of the user access in their respective systems • Optionally the system administrators can be asked to confirm the provisioning or de-provisioning actions they have taken by selecting a checkbox in the user's profile from the MIM Portal • User self-service will allow users to update their cell phone, fax, and office location in the MIM portal	
Group management in AD from the MIM Portal	Design and implement the workflows and synchronization rules used to manage security and distribution groups in AD. Workflows include: • Attribute validation and naming convention enforcement • Approval required when joining certain groups • Group owner notification for extending the group prior to expiration and deletion of the group upon expiration	The number of group attributes built or validated is limited to 3. Group owners will be maintained manually by the group administrators. Group size is limited to less than 25,000 members.
Group management in AD from HR	• Design and implement the workflows to automatically generate dynamic groups based on the imported user data, such as a group is automatically created for each	

	city present in the employee records imported from HR • The membership of these dynamic groups is automatically calculated based on the data imported from HR and AD • Exceptions to these dynamic group memberships is handled by adding users to corresponding Inclusion or Exclusion manual groups • Each of these Inclusion and Exclusion groups can be requested from the MIM Portal and automatically created by MIM	
Dynamic Group conversion	Convert up to 5 groups imported from AD to Dynamic Groups and provide guidance to the Orange County on how to convert the remaining groups	Scope is limited to 5 dynamic groups.
Self-Service Password Reset	Allow the user to update their passwords in a Self-Service Password Reset (SSPR) portal without administrative intervention	County will be responsible for providing the high-availability infrastructure components required to implement MIM SSPR if Azure SSPR is not used.
Bulk Import from a CSV file	Provide a PowerShell script to allow for creating, updating, and deleting user, contact, and group resources in MIM from a CSV file	
High-availability	Plan for high-availability of the different solution components within the overall design	Orange County will be responsible for providing the load balancing solution and for implementing the SQL servers for high-availability.
Test environment	Build the solution in a test environment based on the Functional Specification document	
User acceptance testing (UAT)	Assist the County stakeholders in conducting UAT in the test environment, based on the documented test cases in the Test Plan	UAT will be limited to 10 County business days
Production rollout	• Assist Orange County with the implementation of the solution in the production environment based on the Deployment Guide	Scope is limited to fewer than 50,000 users and 50,000 groups imported from AD. The remediation activities required to fix un-joined

	• Import from AD, all user, contact and group objects to be managed from the MIM Portal • Import from HR all user records and make sure they join with corresponding AD accounts • Validate the changes resulting from the data imported from HR before exporting them to AD Validate the changes resulting from the data imported from AD before exporting them to HR	objects, unwanted changes or other unplanned impacts has an estimated duration of 7 days.
Stabilization of the solution in production	• Assist Orange County in performing UAT in production • Monitor the solution in production to detect and fix any issues that may arise, according to Section 1.2.7: Testing	Stabilization activities in production has an estimated duration of 14 days.
Knowledge Transfer	Provide informal knowledge transfer to the County staff on the solution components implemented.	

1.2.2 Software Products and Technologies

The products listed in the following table are required to deliver this project. Orange County is responsible for obtaining all required licenses and products.

Table 2: Software Products/Technologies Required

Product and Technology Item	Version	Required by Date
SQL Server	2014	Prior to start of project
Microsoft Identity Manager	2016	Prior to start of project

1.2.3 Data Migration

No data migration is expected.

1.2.4 Integration and Interfaces

The implementation of the following MIM Connectors is in scope.

Table 3: Integration Interfaces Scope

Interface	Description of Scope	Responsibility
MIM Service	Out-of-the-box connector used to synchronize data between the MIM Service database and the MIM Synchronization database.	Microsoft
Active Directory	Out-of-the-box connector used to synchronize data between the 27 Orange County AD domains	Microsoft

	and the MIM Synchronization database.	
HR	Out-of-box Database connector used to synchronize data between the Orange County HR system and the MIM Synchronization database.	Microsoft and County
OC Profile	Out-of-box Microsoft SQL Server connector used to synchronize data between the Orange County OC Profile system and the MIM Synchronization database.	Microsoft and County

1.2.5 Environments

The environments listed in the following table are required to deliver this project. The party listed is responsible for establishing the environment in the location specified, by the time noted.

Table 4: Required Environments

Environment	Location	Responsibility	Ready by
Development and Test	County	County	One week prior to the start of Build phase
Production	County	County	One week prior to the start of Deploy phase

The development and test environment must have an instance of AD with similar data as in production. In particular, the following objects need to be the same: Organizational Units, Users, Contacts and Groups.

An instance of the HR system must also be set up in the test environment with data similar to production. Note however that if the County cannot setup the HR system but can provide the backend database, then they should provide a script to perform the operations needed during testing.

1.2.6 Training and Knowledge Transfer

Knowledge transfer is defined as informal activities provided when Orange County team members are working side-by-side with Microsoft. These include, but are not limited to, the following: whiteboard discussions, email threads, conference calls and facilitated meetings on technical topics. No deliverables or meeting summary will be provided for these sessions or activities.

Informal knowledge transfer is a valuable adjunct to, but not a substitute for, formal training. Microsoft recommends that formal training be procured and attended by the technical staff prior to the initiation of this project.

1.2.7 Testing

The following testing is in scope.

Table 5: Testing Scope

Test Type	Description	Responsible	Provides Test Data/Cases	Guidance & Support	Environment
Unit testing	Unit test specific functionality of the individual solution components during the Build process.	Microsoft	Microsoft	Microsoft	Development/Test
Functional testing	Functional testing focuses on the functionality of the solution meeting the design and integration with connected data systems. Test cases are based upon the Functional Specification document.	Microsoft	Microsoft	County	Development/Test
UAT	Test functionality of key County real world scenarios. Testing is based on the test plan where test cases with step-by-step instructions are documented.	County	County	Microsoft	Development/Test; Production

As defects are identified during testing, the defect priority will be jointly agreed upon by the County and Microsoft. Microsoft team will triage the defect and fix all in-scope P1 and P2 defects. Defect priorities are shown in the following table.

Table 6: Defect Priorities

Defect Priority	Description of Priority
P1	Showstopper defect. Development, testing, or production launch cannot proceed until the defect is corrected. Must fix as soon as possible. Defect is blocking further progress in this area. Solution cannot ship and the project team cannot achieve the next milestone.
P2	Defect must be fixed prior to moving to production. Does not affect test plan completion
P3	It is important to correct the defect. However, it is possible to move forward into production using a workaround. Does not impact functionality as designed (for example, message change in user experience program).
P4	Feature enhancement or cosmetic defects. Design change from original concepts.

Note: P3 and P4 defects will be logged and the County may choose to schedule their remediation either by change request, by the **Change Management Process** described in Section 2.4.4 of this Scope of Work (SOW), or during a subsequent release. P3 and P4 defects will not be corrected by default under this SOW.

Note: Product bugs and design change requests are not in scope. Product related issues must be addressed separately through Premier support.

1.3 Areas Out of Scope

Any area that is not explicitly listed in Section 1.2 as within scope is out of scope for this engagement. The areas that are out of scope for this engagement include, but are not limited to, the following:

Table 7: Areas Out of Scope

Area	Description
Integration with additional applications and systems	MIM will be integrated with 27 Active Directory domains, an HR system, and OC Profile database through out-of-box connectors. Five systems of the County choosing will also be integrated but without connectors, meaning that MIM will only send email notifications to their respective system administrators to perform manual provisioning and deprovisioning. Any other additional systems are out of scope.
Advanced user management	Any operation other than creating, updating, or deleting user and contact objects in AD is not in scope. This includes creating and managing user shares, provisioning Microsoft Exchange mailboxes, or setting user permissions on network resources.
Advanced group management	Advanced group management workflows are not in scope. These include, but are not limited to, the following: • Automatic ownership management • Periodic group attestation • Group nesting

	• Empty group notification
Exchange resource management	Management of resources such as mailboxes, contacts, and distribution lists in Microsoft Exchange Online or Exchange on-premises. Contacts and distribution lists will be managed only in AD and will not be tested with Exchange as part of this engagement.
MIM reporting	The MIM reporting component will not be installed as part of the solution, meaning that the ability to track historical actions taken and changes made through MIM will be limited to 30 days only.
Management of tier-0 accounts and groups	The management of tier-0 or administrative user accounts and groups.
Data clean-up	Cleaning the data in AD, including making sure that the attributes imported comply with the data format standard in MIM (such as Mail Nickname, Email and Account Name). This includes the population of the employee ID attribute on all user objects.
Disaster recovery	Implementation of a solution that is geo-resilient.
Custom portal	The development of a custom web portal. Only the default MIM Portal will be customized to the extent of its out-of-box capabilities.
MIM Client Extensions	The deployment of MIM client extensions such as the Outlook add-in to user workstations for request approval or group management.
AD redesign or changes	Any AD redesign or changes to the current AD environment will be the County responsibility.
SQL infrastructure	Implementation of a highly-available SQL infrastructure used by the solution components will be the County responsibility.
Networking	Implementation of firewall changes, load balancer setup, or any other form of networking changes will be the County responsibility.
Hardware	Hardware will not be provided under this SOW. The County is responsible for acquiring all necessary hardware.
Product licenses	Product licenses (Microsoft or non-Microsoft) will not be provided under this SOW. The County is responsible for acquiring all necessary product licenses required as a result of this SOW.
Process re-engineering	Design of functional business components of the solution unless specifically included in scope and delivered by Microsoft Consulting Services (MCS) Operations Consulting staff.
Organizational change management	Design or re-design of the County's functional organization unless specifically included in scope and delivered by MCS Operations Consulting staff.
Formal training	Formal classroom or hands-on lab training.

2. Project Approach, Timeline and Deliverable Acceptance

2.1 Approach

The estimates for this project assume that Microsoft will use the Microsoft Solutions Framework (MSF) to implement each phase within this SOW. MSF represents a world-class solution development approach that provides for well-defined phases that take into account definition of requirements, architectural design, detailed solution design, solution build, solution testing, and managed release cycles of the solution.

2.1.1 Engagement Initiation

Successful delivery and adherence to the schedule defined in this section requires the County to complete the following prior to project kickoff:

- Identify all stakeholders who may have an interest in the project and make sure that they are invited to the kick-off meeting.
- Collect any documentation that may be helpful during the delivery, such as:
    - Business and Technical Requirements, such as:
        - Security policies and standards
        - Standards for server configuration
        - Naming convention for users and groups stored in AD
    - Current Identity and Access Management solution information, including the processes used
    - AD design documentation such as forests, domains, trusts, sites, group policies, and organizational units (OUs)
    - Network diagrams, indicating at a minimum the different local-area networks (LANs), wide-area network (WAN) links, available bandwidth, and any firewall or packet filtering devices
    - Operations information, such as:
        - Backup and restore standards and infrastructure documentation
        - System-monitoring standards and documentation
        - Change Management processes and tools
    - HR data information, such as the attributes present in the HR database and sample data for each. A dump of the HR data in a CSV file is usually very helpful

2.1.2 Envision Phase

During the Envision phase, the team will define the requirements for the overall solution, gain an understanding of the environment, design a high-level solution strategy that meets the requirements, and define the roles and responsibilities of the project team. Microsoft team will create a Vision and Scope document to identify what will be accomplished and align expectations between the project team and stakeholders. The Envision Phase ends when the Vision and Scope document is approved by Orange County. This milestone indicates that the team shares a common vision and agrees on the scope of work necessary to bring the vision to reality.

Table 8: Envision Phase

Category	Description
Microsoft activities	• Project kick-off meeting • Review existing documentation • Conduct Envisioning and Assessment workshops • Discover the current identity and access management processes • Review the AD structure and how user, contact and group objects are stored in each of the 27 in-scope Active Directory domains • Review data attributes which will be pushed to the OCProfile database • Review current processes for maintaining users in HR • Review the schema of the HR database and the user profile information maintained • Collect County business and technical requirements • Validate the project vision statement and project goals • Determine the personas interacting with the solution • Define the identity management use cases • Document the results and findings collected from various stakeholders in the Vision and Scope document
County responsibilities	• Coordinate resources for participation in the Envisioning and Assessment workshops • Facilitate any necessary communication for requests that may result from discussions during the Envisioning and Assessment workshops, including information-gathering exercises • Make available all documentation that may be helpful to the project • Provide all necessary information regarding the existing environment and the systems that are in scope • Participate in the review and approval process of the Vision and Scope document • Procure the necessary hardware or virtual machines for the development/test environment
Exit criteria	• Approval of the Vision and Scope document
Key assumptions	• Orange County stakeholders will be available on a part-time basis to attend the Envisioning and Assessment workshops, answer Microsoft questions, and validate the solution requirements and use cases • During this phase, Microsoft will gather additional information needed for refinement of the in-scope solution. This information will be used during the Plan Phase to complete the solution architecture design • The Vision and Scope document will be written using Microsoft Services templates

Workshops

With County participation, the following workshops will be led by Microsoft during this phase.

Table 9: Workshops

Activity	Topics Covered	Maximum Hours per Session	Maximum Number of Session
Envisioning and Assessment workshops	• Review the current AD environment • Discuss how identities are stored and managed in the 27 in-scope Active Directory domains • Discuss how the OCProfile will be transitioned to a consumer of data from MIM • Discuss HR onboarding/offboarding processes • Discuss how employee information is stored and managed in HR • Collect detailed County requirements for the in-scope identity management processes • Discuss MIM product capabilities • Outline conceptual future state • Discuss other initiatives related to the project	2	5
Document review	• Review Vision and Scope document	2	1

Phase Outputs

The County will provide the following items:

Table 10: Phase Outputs

Name	Description
Decisions	• Validation of the scope, requirements, and use cases for the project
Development and Test Lab	• Hardware and software for the Development/Test lab environment

Microsoft will provide the following Service Deliverables. Those that require formal review and acceptance, as described in Section 2.3 **Service Deliverable Acceptance Process**, are indicated as such.

Table 11: Envision Phase Service Deliverables

Name	**Description**	**Acceptance Required (Y/N)**
Vision and Scope document	Contains a description of the County's situation and needs, the boundary of the solution defined though the range of features and functions, and the solution design strategy that will form the starting point used to create the County's solution. Designs at this stage will be conceptual in nature and will provide input to developing the functional specification. This document includes the project vision, all agreed upon requirements, and a solution design approach.	Y

2.1.3 Plan Phase

During the Plan Phase, Microsoft works through the design and prepares the Functional Specification document and Project Plan. Following the completion of this phase, Microsoft begins the development of the solution in the Build Phase.

Table 12: Plan Phase

Category	**Description**
Microsoft activities	• Facilitate solution design sessions to define how MIM will implement the use cases documented in the Vision and Scope document • Discuss different options with the County database administrators for how to read or write user data to the HR database • Document the logical and physical design of the solution components in the Functional Specification document • Assist the County Project Manager in the creation of the Project Plan • Review the Test lab to make sure it meets the requirements for the project
County responsibilities	• Coordinate resources for participation in design sessions • Make timely decisions about specific design elements • Create the communications and training plan for the project • Participate in the review and approval process of the Functional Specification document • Work with Microsoft resources to create and maintain a Project Plan (work breakdown structure) document • Review and approve the Functional Specification document • Setup AD in the development/test environment with similar data as in production. In particular, the following objects need to be the same: Organizational Units, Users, Contacts and Groups • Setup the HR system in the development/test environment with similar data as in production
Exit criteria	• Approval of the Functional Specification document

Key assumptions	• Orange County will provide necessary technical subject matter experts who will make design decisions • The AD forest setup in the Development/Test Lab contains the same domains, organizational unit structure, users, contacts and groups as the one in production • The HR database setup in the Development/Test Lab contains the same user and department information as in production • Orange County will be responsible for setting up the views, tables, triggers or stored procedures needed by MIM to read and write to the HR database through this connector • The Functional Specification document will be written using Microsoft Services templates • The Project Plan will be in a Work Breakdown Structure (WBS) format using Microsoft Project

Workshops

With County participation, the following workshops will be led by Microsoft during this phase.

Table 13: Workshops

Activity	Topics Covered	Maximum Hours per Session	Maximum Number of Session
Design workshops	• Discuss initial user and group import from AD. • Discuss user management in AD from the MIM Portal. • Discuss group management in AD from the MIM Portal • Discuss how user and department information will be imported from HR for employees, including delta change detection out of the HR database. • Discuss how user and department information will be imported from the MIM Portal. • Discuss how user attributes will be written to HR. • Discuss how the current 12 attributes synchronized to in-scope directories by Unity Sync will be transitioned to MIM.	2	5
Document review	• Functional Specification document	2	1

Phase Outputs

The County will provide the following items:

Table 14: Phase Outputs

Name	Description
Decisions	• Make decisions relative to the design of the proposed solution
Development and Test Lab	• The Development and Test Lab has been setup by Orange County per Microsoft's requirements and is ready for MIM installation.

Microsoft will provide the following Service Deliverables. Those that require formal review and acceptance, as described in Section 2.3 **Service Deliverable Acceptance Process**, are indicated as such.

Table 15: Plan Phase Service Deliverables

Name	Description	Acceptance Required (Y/N)
Functional Specification document	Contains the specification of the logical and physical design for the different components of the proposed solution. This document includes the details of all the configuration settings for the solution components. Someone with MIM skills should be able to reconfigure the solution from scratch using this document.	Y

2.1.4 Build Phase

During the Build Phase, Microsoft refines the baseline design created in the Plan Phase, builds the solution functionalities, and performs unit testing of each use case implemented. Completion of this phase marks the transition to the Stabilize Phase.

Table 16: Build Phase

Category	Description
Microsoft activities	• Install MIM in the Development/Test Lab. • Configure the management agent and synchronization rules for the MIM Service connector. • Configure the management agent and synchronization rules for the AD connectors to the 27 in scope Active Directory forests. • Configure the management agent and synchronization rules for the Generic SQL connector used for HR connectivity. • Configure the management agent and synchronization rules for the SQL Server connector used for OCProfile connectivity. • Configure the Sets, Workflows, and Management Policy Rules (MPRs) to model the identity management processes based on the requirements and use cases documented in the Vision & Scope document. • Customize the MIM Portal. • Conduct unit testing, fix issues found, and retest solution components.

	• Draft the Test Plan describing the test environment and containing all test cases required to validate the requirements and use cases documented in the Vision & Scope document. • Develop the Deployment Guide document.
County responsibilities	• Coordinate resources for participation in the Build activities. • Setup the tables, views, triggers or stored procedures as requested by Microsoft for the HR Generic SQL Connector. • Assist with the definition of the test cases for the solution. • Review and approve the Test Plan document. • Review and approve the Deployment Guide document.
Exit criteria	• Solution is built and prepared for testing. • Approval of the Deployment Guide document • Approval of the Test Plan document
Key assumptions	• Microsoft team will have access to user accounts that are granted administrative privileges on all servers where the solution components are installed in the Development/Test Lab. • The Test Plan and Deployment Guide documents will be written using Microsoft Services templates. • Prior to the start of the Build phase the County must have set up an instance of their HR application and its back-end database in their development/test environment. This database must mirror the one in production. Note that if the HR application cannot be installed in the development/test environment, the County should instead provide scripts to directly add/update/delete records in the HR database for testing purpose. • Up to two "MIM Service" and one "MIM Synchronization Service" components will be implemented in each one of the two environments: Development/Test and Production.

Phase Outputs

Microsoft will provide the following Service Deliverables. Those that require formal review and acceptance, as described in Section 2.3 **Service Deliverable Acceptance Process**, are indicated as such.

Table 17: Build Phase Service Deliverables

Name	Description	Acceptance Required (Y/N)
Deployment Guide document	This document describes the steps to install and configure MIM in the production environment.	Y
Draft Test Plan	A draft document that describes test objectives, test methodologies and tools, expected results, responsibilities, and resource requirements. It details all test cases for the solution and is provided in draft format until the test cases have been implemented during the Stabilize Phase.	Y

2.1.5 Stabilize Phase

During the Stabilize Phase, Microsoft conducts testing and focuses on resolving issues and bugs to prepare the solution for release. Completion of this phase marks the transition to the Deploy Phase.

Table 18: Stabilize Phase

Category	Description
Microsoft activities	• Perform functional testing of the solution built in the test environment. • Adjust solution design and configuration settings as appropriate. • Assist County in the completion of UAT per the test cases documented in the test plan. • Update the test plan document based on actual results of the testing. • Conduct knowledge transfer about the solution built to the County.
County responsibilities	• Begin scheduling for the production deployment. • Provide staff to assist with UAT testing of the solution. • Conduct UAT and provide test results to Microsoft team. • Review and approve the test plan updated with the test results.
Exit criteria	• Acceptance of the test results from the Test Plan, authorizing the deployment of the solution into the production environment.
Key assumptions	• Orange County will perform all UAT activities and Microsoft will provide assistance as needed.

Phase Outputs

The County will provide the following items:

Table 19: Phase Outputs

Name	*Description*
Test results	Test results at the completion of UAT.

Microsoft will provide the following Service Deliverables. Those that require formal review and acceptance, as described in Section 2.3 **Service Deliverable Acceptance Process**, are indicated as such.

Table 20: Stabilize Phase Service Deliverables

Name	Description	Acceptance Required (Y/N)
Final Test Plan	The final test plan includes all the test results and notes that were captured for each test case executed during UAT. This document is used as an approval mechanism for implementing the solution into the production environment.	Y

2.1.6 Deploy Phase

During the Deploy Phase, Microsoft conducts the activities needed to deliver the solution in the production environment. The Deploy Phase includes the monitoring and stabilization of the solution while transitioning it to the operations and support Microsoft teams before project close out.

Table 21: Deploy Phase

Category	Description
Microsoft Activities	• Conduct a one-hour Assessment Workshop to assess Orange County readiness to operate and maintain the solution in production. • Assist Orange County with the deployment of the solution to production per the Deployment Guide. • Initially import and aggregate the data from HR and AD into MIM. • Remediate the un-joined objects and the unwanted changes before exporting the changes to AD or HR. Note that this activity is time boxed to 3 days. • Assist Orange County in conducting UAT in production. • Monitor, troubleshoot, and fix issues that result from the use of the solution in the production environment. • Update the Functional Specification document with the final design and configuration settings. • Conduct a project close-out meeting to wrap up the engagement and share lessons learned.
County Responsibilities	• Participate in the Assessment Workshop and confirm that the solution is ready for deployment. • Provide relevant personnel needed for deployment, operations, and support. • Participate in the project close-out meeting.
Exit Criteria	• Acceptance of the test results from the test plan completed in production.
Key Assumptions	• Stabilization activities in production is limited to 10business days. • After the initial import from Active Directory, any change made directly to the users, contacts and groups in Active Directory will get overwritten by MIM.

2.2 Timeline

It is estimated that this engagement will be performed according to the timeline depicted below and will include the phases and milestones noted. The project will start on the date mutually agreeable by both parties subsequent to the full execution of this Agreement. No party shall unreasonably delay the start of the project. The actual timeline for this engagement will be relative to the project start date, and all dates and durations provided are estimates only.

The diagram below outlines the timeline for this engagement:

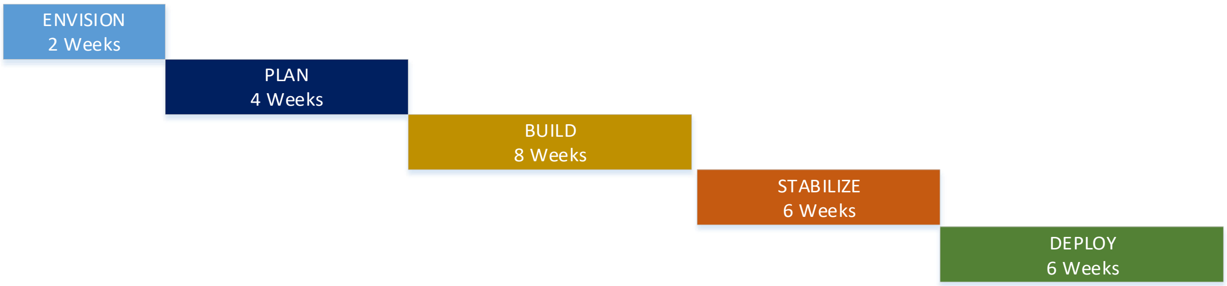


Figure 1: Project Timeline

2.3 Service Deliverable Acceptance Process

At specified milestones throughout the project, Microsoft will submit completed project service deliverables for County's review and approval. Service deliverables will fall into the following categories:

1. Document deliverables (for example, Word, Excel, Visio, or Project).
2. Functioning components or solution deliverables (such as custom source code).

The County's use or partial use of a service deliverable will constitute acceptance of that Service Deliverable. The County may provide its acceptance or rejection of deliverables electronically through email. The following details the acceptance process for each of the deliverable types.

Document deliverables: within five business days from the date of submittal, the County must either:

- Accept the document deliverable by signing, dating, and returning the Service Deliverable Acceptance Form

  OR

- Provide a written notice rejecting the document deliverable, including a single and complete list describing every reason for rejection.

The following assumptions also apply:

- Document deliverables shall be deemed accepted unless County provides five business day written rejection notice as described previously.
- Microsoft will correct problems with a document deliverable that are identified in the written rejection notice, as described above, and within the scope of this SOW, after which the document deliverable will be deemed accepted.
- Issues that are outside the scope of this SOW and feedback provided after a document deliverable has been deemed accepted will be addressed as a potential change of scope pursuant to the Change Management Process outlined in this SOW.

Functioning components or solution deliverables: the functioning solution is typically comprised of configured commercial software and custom source code and associated objects. Review and acceptance of the solution or custom source code, for this SOW only, is based on completion and signoff of the defined County acceptance test.

2.4 Project Governance Approach

This section outlines the project governance structure and processes to which Microsoft team will adhere for this engagement.

2.4.1 Part-Time Project Management

This project will be managed by a part-time Microsoft Project Manager based on a commitment of up to **8 hours** per week. Prior to the start of the engagement, a mutually agreed to coverage plan or meeting schedule will be documented in writing. As this resource is part-time, the following operational constraints are assumed:

Table 22: Project Management Activities

Activity	Description
Communications	• Provide one weekly status report or a bi-weekly status report if project is delivered at less than full-time cadence. • Prepare and lead one status meeting per week of no more than one hour in duration or bi-weekly meeting if project is delivered at less than full-time cadence • Remotely attend or participate in one steering committee meeting per month. Note: not all County meetings will be attended.
Scope management and change control	• Attend one scope meeting per week remotely. • Manage project change control.
Finance	• Provide weekly (or bi-weekly as noted above) financial report as part of the status report.
Schedule	• Manage the schedule for the MCS scope of work and MCS resources.
Human resources and staff management	• Coordinate MCS resources (only), including staffing, task assignments, and status reporting.

The scope of Microsoft part-time project management service is limited to managing MCS and Microsoft partners who are subcontracted through MCS.

Microsoft will provide project management for the duration that is defined in theScope of Work . Changes to this duration or to the amount of hours per week will be handled by the change management process.

2.4.2 Communication Plan

The following will be used to provide formal communication during the course of the project:

- Microsoft Project Manager, working in conjunction with the County Project Manager, will document a detailed communication plan as part of the master project management plan and will compile status reports for distribution to both County and Microsoft.
- Weekly status meetings will be held to review the project's overall status, the acceptance of deliverables, the project schedule, and open issues noted in the status report.

2.4.3 Issue/Risk Management Procedure

The following general procedure will be used to manage active project issues and risks during the project:

- **Identify**: Identify and document project issues (current problems) and risks (potential events that impact the project)
- **Analyze and prioritize**: Assess the impact and determine the highest priority risks and issues that will be managed actively
- **Plan and schedule**: Decide how high-priority risks are to be managed and assign responsibility for risk management and issue resolution
- **Track and report**: Monitor and report the status of risks and issues and communicate issue resolutions
- **Control:** Review the effectiveness of the risk and issue management actions

Active issues and risks will be monitored and reassessed on a weekly basis.

2.4.4 Change Management Process

During the project, either party may request in writing additions, deletions, or modifications to the services described in this SOW (“Change Request”).

For all change requests, regardless of origin, Microsoft will submit to the County the Microsoft standard Change Request Form, which will describe the proposed changes to the project, including the impact of the changes on the project scope, schedule, fees, and expenses.

For all change requests originated by the County, Microsoft will have a minimum of 3 business days from receipt of the change request to research and document the proposed change and prepare the Change Request Form.

The County will have 3 business days from your receipt of a completed Change Request Form to accept the proposed changes by signing and returning the Change Request Form. If the County does not sign and return the Change Request Form within this time period, the change request will be deemed rejected and Microsoft will not perform the proposed changes.

No change to this project will be made unless it is requested and accepted in accordance with the process described in this section. Microsoft will have no obligation to perform or commence work in connection with any proposed change until a Change Request Form is approved and signed by the designated project managers from both parties. Notwithstanding anything to the contrary, Change Request shall be deemed to be invalid unless it is in written and approved, as necessary, by the County’s Board of Supervisors prior to commencement of the work requested.

2.5 Project Completion

Microsoft will provide services defined in this SOW to the extent of the funding for hours of services and period of performance specified in the Scope of Work. If the County requires additional services, a modification to the contract will be completed by the parties adding funding through the Change Management Process.

The project will be considered complete when any of the following conditions are met:

1. All of the service deliverables identified within this SOW and any change requests accepted, pursuant to the change management process defined in this document, have been delivered and accepted or deemed accepted.
2. The fee provisions of the Scope of Work have been met.

3. The term of the Agreement has expired.
4. This SOW is terminated pursuant to the provisions of the Agreement.
5. The Work Order has been terminated.

3 Project Organization and Staffing

3.1 Project Organization Structure

This section describes the overall project organization structure, reporting relationships, and key project roles.

The project will be organized as depicted in the following diagram.

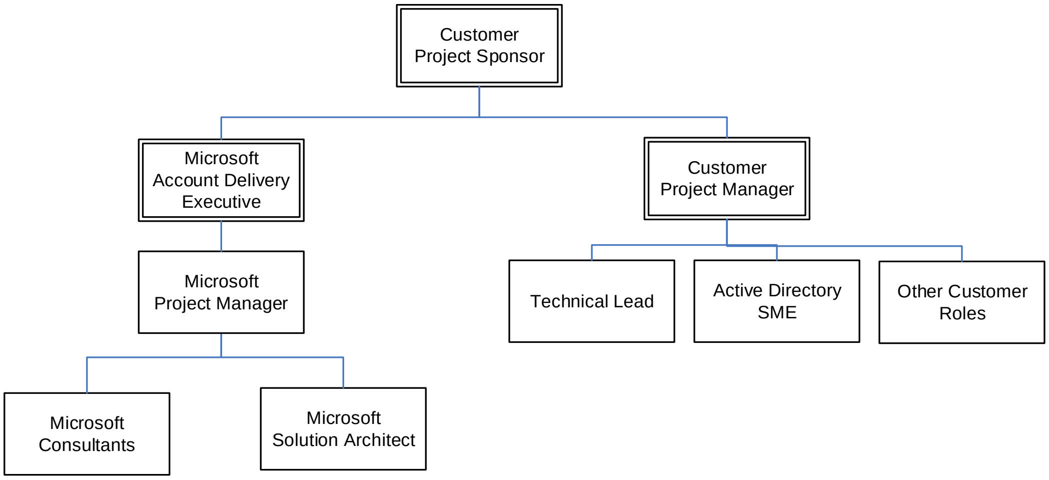


Figure 2: Project Organization Structure

3.2 Project Roles and Responsibilities

This section provides a brief description of key project roles and responsibilities.

3.2.1 County Project Roles and Responsibilities

Table 23: County Roles and Responsibilities

Role	Responsibilities	Project Commitment
County Project Sponsor	• Makes key project decisions, serves as a point of escalation, and clears project roadblocks.	Part-time
County Project Manager	• Primary point of contact for Microsoft team. • Responsible for managing and coordinating the overall project and delivering to schedule. • Responsible for County resource allocation, risk management, project priorities, and communication to executive management. • Coordinates decisions within three business days, or otherwise agreed timeline.	Part-time
Technical Lead	• Primary technical point of contact for the team that is responsible for technical architecture and identity management processes.	Part-time
AD Subject Matter Expert (SME)	• A SME on the current AD implementation at Update [County Name] in Doc Properties.	Part-time
Other County roles	• Other stakeholder from Orange County working with Microsoft team to provide information about the current environment and express their requirements for the project.	Part-time

3.2.2 Microsoft Project Roles and Responsibilities

Table 24: Microsoft Roles and Responsibilities

Role	Responsibilities	Project Commitment
Account Delivery Executive	• Responsible for managing and coordinating the overall Microsoft project • Single point of contact for escalations, billing issues, personnel matters, contract extensions • Facilitates project governance activities, leading the Executive Steering Committee	Part-time
Project Manager	• Responsible for managing and coordinating the Microsoft project delivery • Responsible for issue and risk management, change management, project priorities, and weekly status communication and weekly status meeting • Coordinates only MCS resources and partners subcontracted to MCS, including staffing, task assignments and status reporting	Part-time

Solution Architect	• Responsible for overall solution design • Provides technical oversight. • Verifies that Microsoft recommended practices are followed. • Sets operational criteria for release to production.	Part-time
Consultant	• Assists with the solution design. • Builds and configure the solution components. • Performs unit and functional testing. • Assists County in performing UAT and deploying the solution to production. • Conducts knowledge transfer. • Produces all project deliverables.	Full-time

4 General County Responsibilities and Project Assumptions

4.1 General County Responsibilities

Delivery of Microsoft services depends upon the following County responsibilities, among other items:

- The County will provide suitable work spaces with desks, chairs, telephones.
- The County will provide LAN connections giving Microsoft onsite team access to the Internet and email.
- The County will provide access to all necessary County work sites, systems logon, passwords, and material and resources as needed and as advised by Microsoft in advance.
- The County will assume responsibility for management of all non-Microsoft managed vendors.
- The County will provide access with proper licenses to all necessary tools and third-party products required for Microsoft to complete its assigned tasks.
- The County will acquire and install the appropriate server capacity required to support the environments as defined in the scope section of this SOW.
- The County will provide accurate and complete information, as needed.
- The County will take timely decisions and obtain approvals from management, as needed.
- The County will provide Project Management.

4.2 Project Assumptions

The Services, fees, and delivery schedule for this project are based on the following assumptions:

1. The standard work day for the project is between 8:00 AM and 5:00 PM PT local time where the team is working, Monday through Friday, except for scheduled holidays.
2. In performing services under this SOW, Microsoft will rely upon any instructions, authorizations, approvals, or other information provided by the County's Project Manager or personnel duly designated by the County's Project Manager. All estimates regarding fees, timelines, and our detailed solution are based on information provided by the County to date.
3. Microsoft's resources and Microsoft subcontractors' resources may perform services remotely or onsite from Microsoft facilities, County facilities, or Microsoft partner's facilities.

4. Informal knowledge transfer will be provided throughout the project. Informal knowledge transfer is defined as the County’s staff working alongside Microsoft. No formal training materials will be developed or delivered as part of informal knowledge transfer.
5. If the project schedule requires Microsoft resources or Microsoft subcontractors’ resources to perform dedicated services at the County’s site on a weekly basis, Microsoft resources will typically be onsite for three nights and four days; arriving on Mondays and leaving on Thursdays.

ATTACHMENT C
COMPENSATION AND PAYMENT

I. **Compensation:** Microsoft agrees to provide services at the fixed rates and prices as set forth in the Master Agreement. The total amount of this Agreement shall not exceed **$489,709.00** and a work orders up to an additional amount of $200,00.00. The County shall have no obligation to pay any sum in excess of this amount unless authorized by written amendment signed by both parties.

Microsoft shall bill County for goods and services provided according to the rates listed below:

Agreement not to exceed $489,709.00 & work orders up to $200,000.00

Classification/Title	Unit	Published Hourly Rates	Fully-Burdened Rates*
Architectural Consultant	Hour	$305.00	$344.00
Principal Consultant	Hour	$292.00	$331.00
Senior Consultant	Hour	$279.00	$335.00
Project Manager	Hour	$268.00	$307.00
Account Delivery Executive*	Hour	$268.00	$307.00
Consultant*	Hour	$250.00	$308.00
Associate Consultant	Hour	$217.00	$277.00
Technician V	Hour	$260.00	$310.00
Technician IV	Hour	$245.00	$295.00
Technician III	Hour	$216.00	$266.00
Technician II	Hour	$189.00	$239.00
Technician I	Hour	$163.00	$186.00
Technician	Hour	$136.00	$158.00
Offshore Global Delivery Consultant	Hour	$75.00	$75.00

*The totals referenced above were calculated using fully-burdened rates for Microsoft Resources. The services component of these fully-burdened rates is equal to “Published Hourly Rates” from Microsoft’s Public Sector Services Published Price List for FY18. These fully-burdened rates, provided at Orange County’s request, are in compliance with all of its procurement policies, laws, rules and regulations. Fully Burdened Rates include travel expenses.

II. **Payment Terms:** Payment shall be made in ARREARS. Payment will be net forty-five (45) days after receipt of an invoice in a format acceptable to the County of Orange. County shall be billed on a monthly basis and shall be verified and approved by the County subject to routine processing requirements. The responsibility for providing an acceptable invoice to the County for payment rests with Microsoft. Incomplete or incorrect invoices are not acceptable and will be returned to Microsoft for correction.

Billing shall cover goods and services not previously invoiced. Microsoft shall reimburse the County of Orange for any monies paid to Microsoft for good and services not provided or when goods and services do not meet the Agreement requirements. County reserves the right to terminate this

Agreement for cause if Microsoft does not meet the applicable specification for the Scope of Work identified in Attachment A.

Payments made by the County shall not preclude the right of the County from thereafter disputing any goods involved or billed under this Agreement and shall not be construed as acceptance of any part of the goods.

III. Invoice Instructions: Each invoice must be on Microsoft's letterhead and have a unique number and shall include the following information:

a. Microsoft's name and address
b. Microsoft's remittance address
c. County Agreement #MA-017-19010780
d. Microsoft's Federal I.D. number
e. Date of Order/Service date(s)
f. Product/service description, quantity, prices
g. Total invoice amount

Invoices are to be forwarded to:

County of Orange
OCIT/Budget & Finance Division
Attention: Accounts Payable
1055 N. Main Street, 6th Floor
Santa Ana, CA 92701

ATTACHMENT D
MICROSOFT BUSINESS ASSOCIATE AGREEMENT

SEE SEPARATE ATTACHMENT TITLED
“MICROSOFT SERVICES BUSINESS ASSOCIATE”

Microsoft Services
Business Association Amendment

Microsoft Business and
Services Agreement number

This Business Associate Amendment (this “Amendment”) is entered into between the Parties identified on the signature form (individually, a “Party” and, collectively, the “Parties”). It supplements the ***[insert as applicable Microsoft Services Agreement or Microsoft Business and Services Agreement]*** (the “Services Agreement”).

This Amendment is applicable only to “Services” as that term is defined in the Services Agreement. Services do not include, and this Amendment is not applicable to, “Online Services,” which means the Microsoft hosted services identified in the Online Services section of the Microsoft product list.

The Services provided to Customer may require Microsoft to create, receive, maintain, or transmit Protected Health Information. Customer is a Covered Entity, a Health Care Component of a Hybrid Entity, Organized Health Care Arrangement (or OHCA) or a Business Associate. To the extent Microsoft creates, receives, maintains, or transmits Protected Health Information, Microsoft is a Business Associate of Customer. As such, HIPAA requires Microsoft and Customer to comply with additional obligations under the Privacy Rule, Breach Notification Rule, and Security Rule that relate to the Use, access, and Disclosure of Protected Health Information.

The terms and conditions in this Amendment supersede any conflicting terms and conditions in the Services Agreement and supersede and replace any previous Services Agreement amendments related to the subject matter of this Amendment. The Parties amend the Services Agreement with the following:

1. *Definitions.*

Except as otherwise defined in this Amendment, any and all capitalized terms shall have the definitions set forth in HIPAA, and the Services Agreement.

“**Breach Notification Rule**” means the Breach Notification for Unsecured Protected Health Information Final Rule in 45 CFR § 164.410.

“**Business Associate**” shall have the same meaning as the term “business associate” in 45 CFR 160.103 of HIPAA.

“**Covered Entity**” shall have the same meaning as the term “covered entity” in 45 CFR § 160.103 of HIPAA.

“**Customer**” means the customer identified on the signature form.

“**HIPAA**” collectively means the administrative simplification provision of the Health Insurance Portability and Accountability Act enacted by the United States Congress, and its implementing regulations, including the Privacy Rule, the Breach Notification Rule, and the Security Rule, as amended from time to time, including by the Health Information Technology for Economic and Clinical Health Act and by the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule.

"**Services**" for this Amendment shall have the same definition as set forth in the Services Agreement.
"Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information.

"**Protected Health Information**" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103 of HIPAA, provided that it is limited to such protected health information that is received by Microsoft from, or created, received, maintained, or transmitted by Microsoft on behalf of, Customer.

"**Security Rule**" means the Security Standards for the Protection of Electronic Protected Health Information.

2. Permitted Uses and Disclosures of Protected Health Information.

a. **Performance of the Microsoft Services Agreement for Microsoft Professional Services.** Except as otherwise limited in this Amendment, Microsoft may Use and Disclose Protected Health Information for, or on behalf of, Customer as specified in the Services Agreement.

b. **Management, Administration, and Legal Responsibilities.** Except as otherwise limited in this Amendment, Microsoft may Use and Disclose Protected Health Information for the proper management and administration of Microsoft and/or to carry out the legal responsibilities of Microsoft, provided that any Disclosure may occur only if: (1) Required by Law; or (2) Microsoft obtains written reasonable assurances from the person to whom the Protected Health Information is Disclosed that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and the person notifies Microsoft of any instances of which it becomes aware in which the confidentiality of the Protected Health Information has been breached.

3. Responsibilities of the Parties with Respect to Protected Health Information.

a. **Microsoft's Responsibilities.** To the extent Microsoft is acting as a Business Associate, Microsoft agrees to the following:

(i) Limitations on Use and Disclosure. Microsoft shall not Use and/or Disclose the Protected Health Information other than as permitted or required by the Services Agreement and/or this Amendment or as otherwise Required by Law; provided that any such Use or Disclosure would not violate HIPAA if done by Customer, unless expressly permitted for Business Associates under HIPAA at 45 CFR § 164.504(e)(2)(i). Microsoft shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request.

(ii) Safeguards. Microsoft shall: (1) use reasonable and appropriate safeguards to prevent inappropriate Use and Disclosure of Protected Health Information other than as provided for in this Amendment; and (2) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.

(iii) Reporting. Microsoft shall report to Customer: (1) any Use and/or Disclosure of Protected Health Information that is not permitted or required by this Amendment of which Microsoft becomes aware; (2) any Security Incident of which it becomes aware, provided that notice is hereby deemed given for Unsuccessful Security Incidents and no further notice of such Unsuccessful Security Incidents shall be given; and/or (3) any Breach of Customer's Unsecured Protected Health Information that Microsoft may discover (in accordance with 45 CFR § 164.410 of the Breach Notification Rule). Notification of a Breach will be made without unreasonable delay, but in no event more than five (5) calendar days after discovery of a Breach. Taking into account the level of risk reasonably likely to be presented by the Use, Disclosure, Security Incident, or Breach, the timing of other reporting will be made consistent with Microsoft's and Customer's legal obligations. Microsoft will (a) investigate the Security Incident or Breach and provide Customer with detailed information about such Security Incident or Breach; and (2) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident or Breach. For purposes of this Section, "Unsuccessful Security Incidents" mean, without limitation, pings and other broadcast attacks on Microsoft's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, as long as no such incident results in unauthorized access, acquisition, Use, or Disclosure of Protected Health Information. Notification(s) under this Section, if any, will be delivered to contacts identified by Customer pursuant to Section 3b(ii) (Contact Information for Notices) of this Amendment by any means Microsoft selects, including through e-mail. Microsoft's obligation to report under this Section is not and will not be construed as an acknowledgement by Microsoft of any fault or liability with respect to any Use, Disclosure, Security Incident, or Breach.

(iv) Subcontractors. In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2) of HIPAA, Microsoft shall require its Subcontractors who create, receive, maintain, or transmit Protected Health Information on behalf of Microsoft to agree in writing to: (1) the same or more stringent restrictions and conditions that apply to Microsoft with respect to such Protected Health Information; (2) appropriately safeguard the Protected Health Information; and (3) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.

(v) Disclosure to the Secretary. Microsoft shall make available its internal practices, records, and books relating to the Use and/or Disclosure of Protected Health Information received from Customer to the Secretary of the Department of Health and Human Services for purposes of determining Customer's compliance with HIPAA, subject to attorney-client and other applicable legal privileges.

(vi) Access. If Microsoft maintains Protected Health Information in a Designated Record Set for Customer, then Microsoft, at the request of Customer, shall make access to such Protected Health Information available to Customer in accordance with 45 CFR § 164.524 of the Privacy Rule.

(vii) Amendment. If Microsoft maintains Protected Health Information in a Designated Record Set for Customer, then Microsoft, at the request of Customer, shall make available such Protected Health Information to Customer for amendment and incorporate any reasonably requested amendment in the Protected Health Information in accordance with 45 CFR § 164.526 of the Privacy Rule.

(viii) Accounting of Disclosure. Microsoft, at the request of Customer, shall make available to Customer such information relating to Disclosures made by Microsoft as required for Customer to make any requested accounting of Disclosures in accordance with 45 CFR § 164.528 of the Privacy Rule.

(ix) Performance of a Covered Entity's Obligations. To the extent Microsoft is to carry out a Covered Entity obligation under the Privacy Rule, Microsoft shall comply with the requirements of the Privacy Rule that apply to Customer in the performance of such obligation.

b. Customer Responsibilities.

(i) No Impermissible Requests. Customer shall not request Microsoft to Use or Disclose Protected Health Information in any manner that would not be permissible under HIPAA if done by a Covered Entity (unless permitted by HIPAA for a Business Associate).

(ii) Contact Information for Notices. Customer hereby agrees that any reports, notification, or other notice by Microsoft pursuant to this Amendment may be made electronically. Customer shall provide contact information to Microsoft as provided in the Services Agreement or such other location or method of updating contact information as Microsoft may specify from time to time and shall ensure that Customer's contact information remains up to date during the term of this Amendment. Contact information must include name of individual(s) to be contacted, title of individuals(s) to be contacted, e-mail address of individual(s) to be contacted, name of Customer organization, and, if available, either contract number or subscriber identification number.

4. Term and Termination.

a. Term. This Amendment shall continue in effect until the earlier of (1) termination by a Party for breach as set forth in Section 4b, below, or (2) expiration of the Services Agreement.

b. Termination for Breach. Either Party immediately may terminate the Services Agreement if the other Party is in material breach or default of any obligation in this Amendment that is not cured within thirty (30) calendar days from written notice of such breach or default.

c. Return, Destruction, or Retention of Protected Health Information Upon Termination. Upon expiration or termination of this Amendment, Microsoft shall return or destroy all Protected Health Information in its possession, if it is feasible to do so, and as set forth in the applicable termination provisions of the Services Agreement. If Microsoft determines that it is not feasible to return or destroy any portions of the Protected Health Information upon termination of this Amendment, then Microsoft shall extend the protections of this Amendment, without limitation, to such Protected Health Information and limit any further Use or Disclosure of the Protected Health Information to those purposes that make the return or destruction infeasible for the duration of the retention of the Protected Health Information.

5. Miscellaneous.

a. Interpretation. The Parties intend that this Amendment be interpreted consistently with their intent to comply with HIPAA and other applicable federal and state law. Except where this Amendment conflicts with the Services Agreement, all other terms and conditions of the Services Agreement remain unchanged. The Parties agree that, in the event an inconsistency exists between the Services Agreement and this Amendment, the provisions of this Amendment will control to the extent of such inconsistency. Any captions or headings in this Amendment are for the convenience of the Parties and shall not affect the interpretation of this Amendment.

b. Amendments; Waiver. This Amendment may not be modified or amended except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, as a bar to, or as a waiver of any right or remedy as to subsequent events.

c. No Third Party Beneficiaries. Nothing express or implied in this Amendment is intended to confer, nor shall anything in this Amendment confer, upon any person other than the Parties, and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

d. **Counterparts.** This Amendment may be executed in counterparts, each of which shall be deemed an original.

e. **Severability.** In the event that any provision of this Amendment is found to be invalid or unenforceable, the remainder of this Amendment shall not be affected thereby, but rather the remainder of this Amendment shall be enforced to the greatest extent permitted by law.

Customer	Microsoft
Name Orange County Information Technology	**Microsoft Corporation ("Microsoft")**
Signature Annie Pham	Signature DocuSigned by: Charlie Brown on behalf of 3174789F577F4E9...
Printed Name Annie Pham	Printed Name David T. Gallagher
Printed Title Procurement Contract Specialist	Printed Title Director of Contracts
Signature Date 5/9/19	Effective Date 3/29/2019

ATTACHMENT E
CYBERSECURITY BEST PRACTICES MANUAL

SEE SEPARATE ATTACHMENT TITLED
“CYBERSECURITY BEST PRACTICES MANUAL”

County of Orange
Cybersecurity Best Practices Manual

Revision History

Date	Revision Scope	Author	Description

Policy Approval

This Cybersecurity Best Practices Manual was prepared by the CyberSecurity Joint Task Force and approved by the IT Executive Council at its August 21, 2018, meeting.

We have approved this Cybersecurity Best Practices Manual as reasonably designed to enable the County of Orange and County departments to address their cybersecurity obligations for County information assets.

Frank Kim
County Executive Officer

Joel Golub

Joel Golub
CEO-Chief Information Officer

Acknowledgement

This manual was developed collaboratively by the CyberSecurity Joint Task Force chaired by the Chief Information Security Officer, Jake Margolis. OCIT is pleased to acknowledge the following task force members for their efforts in the development of the County Cybersecurity Best Practices Manual:

Adil Siddiqui, Health Care Agency
Anna Peters, Health Care Agency
Becky Juliano, OC Public Works
Bill Bauer, Clerk of the Board of Supervisors
Brian Rayburn, OC Community Resources
Bryan Berea, CEO/Risk Management
Carlo Wiseman, Social Services Agency
Charles Ko, OC Sheriff Department
Clyde Gamboa, OC Information Technology
David Castellanos, Health Care Agency
George Singletary, Assessor
Hiren Patel, CEO/Human Resources
Ian Rudge, Child Support Services
Jenny Qian, District Attorney
Jerry Soto, OC Sheriff Department
John Cleveland, County Counsel
Justin Berardino, Registrar of Voters
Kirk Wilkerson, OC Sheriff Department
Lawrence L., OC Sheriff Department
Linda Le, OC Information Technology
Lisa Do, OC Information Technology
Mark Khanlar, OC Information Technology
Mike Hirad, Registrar of Voters
Peter Nguyen, OC Information Technology
Phil Daigneau, Auditor-Controller
Rahul Gupta, District Attorney
Robin Russell, Treasurer Tax Collector
Scott Kim, Auditor-Controller/Internal Audit
Stephen Rivers, County Counsel
Susie Sullivan, Clerk-Recorder
Tiffany Do, OC Information Technology
Valerie Sanchez, Clerk of the Board of Supervisors
Wilson Crider, OC Information Technology

Alan Young, Auditor-Controller
Antonio Castillo, Child Support Services
Betty Stallworth, Auditor-Controller/Internal Audit
Billy Chan, District Attorney
Brian Wayt, OC Sheriff Department
Bryan Prieto, Probation
Carolyn McInerney, County Executive Office
Cindy Pisarski, CEO/Risk Management
Dana Ohanesian, Clerk Recorder
Diana Hantsche, Public Defender
Grady Howe, Social Services Agency
Hugo Ortega, Social Services Agency
Jason Brown, County Counsel
Jerry Sakelaris, Public Defender,
Jimmy Nguyen, Auditor-Controller/Internal Audit
Julie Nguyen, OC Information Technology
Kim Golden, Registrar of Voters
Larry Stansifer, OC Public Works
Lilly Simmering, County Executive Office
Linh Ly, County Executive Office
Lisa Smith, OC Waste & Recycling
Massoud Shamel, County Counsel
Monique Johnson, Child Support Services
Peter Perera, Public Defender
Rachael Vargas, Child Support Services
Ramin Abolfathi, OC Sheriff Department
Scott Holstein, OC Information Technology
Sheila Carter, OC Information Technology
Steve Cote, Auditor-Controller
Thea Bullock, OC Community Resources
Todd Graham, Probation
Will Bogdan, OC Sheriff Department
Zafar Chaudary, Clerk-Recorder

This Page Left Intentionally Blank

Table of Contents

This Page Left Intentionally Blank

1 Introduction

In the current technology dependent business environment, organizations need to anticipate threats, continue essential activities in adverse conditions, and restore mission-critical functions quickly. The successful organization has the ability to evolve so that the impact of incidents are minimized. In addition to information security, disaster recovery, business continuity and crisis management, the resilient organization will integrate risk assessment, mitigation, and incident response into the planning process and daily operations. Individual protective capabilities and plans need to be integrated into a more holistic approach to be part of the organizational norms and practices. The ability to protect the enterprise from cyber hazards and sustain essential functions is the foundation of the cyber resilient organization.

1.1 National Institute of Standards & Technology

The National Institute of Standards & Technology (NIST) is responsible for developing information security standards and guidelines, and the County has chosen to utilize its publications in developing and implementing the County’s cybersecurity programs, policies, and procedures.

Specification of security controls for a system is part of an organization-wide information security program designed to manage organizational risk. The security controls should be rigorous enough to reduce risk while flexible enough for the operation of a system. The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for a system---the security controls necessary to protect individuals and the operations and assets of the organization. The County has chosen the NIST Special Publication 800-53 Revision 4 as its basis for selecting security controls.

1.2 Purpose

The Cybersecurity Best Practices Manual provides a framework and describes best practices to establish a secure environment that safeguards the confidentiality, integrity and availability of the data and information systems used to manage the services provided by the County. IT was designed to comply with applicable laws, regulations and standards. See Appendix K for a listing applicable laws, regulations and standards. **This document provides best practices for departments to use in developing, implementing and maintaining their Departmental Cybersecurity Programs.**

1.3 Authority

The Cybersecurity Best Practices Manual was developed by the Cybersecurity Joint Task Force (CSITF) as stated in the task force’s Charter. The CSITF was created under the IT Executive Council to address the increasing threats to the security of County data and information systems.

1.4 Scope

This Cybersecurity Best Practices Manual applies to all departments in the County. Departments shall implement a Cybersecurity Program that consists of policies, procedures, plans, and guidelines for safeguards to protect information during storage, use or in transit.

1.4.1 Compliance Measurement

An entity designated by the County shall verify compliance to this Cybersecurity Best Practices Manual through various methods, including but not limited to, periodic physical inspection, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

1.4.2 Variances

Variances to this Cybersecurity Best Practices Manual shall be documented and approved following the *County Variance Review & Approval Process*.

1.4.3 Non-Compliance

Non-compliance with this Cybersecurity Best Practices Manual may result in significant delays to the implementation of information systems and/or technologies.

1.4.4 Cybersecurity Best Practices Manual Control and Maintenance

The County Chief Information Security Officer (CISO) is responsible for maintaining this Cybersecurity Best Practices Manual. The County Executive Officer (CEO) shall approve any modifications to this Manual and any related documents. This Manual shall be reviewed at least annually and any revisions approved by the CEO. Questions regarding this Manual should be directed to the CISO.

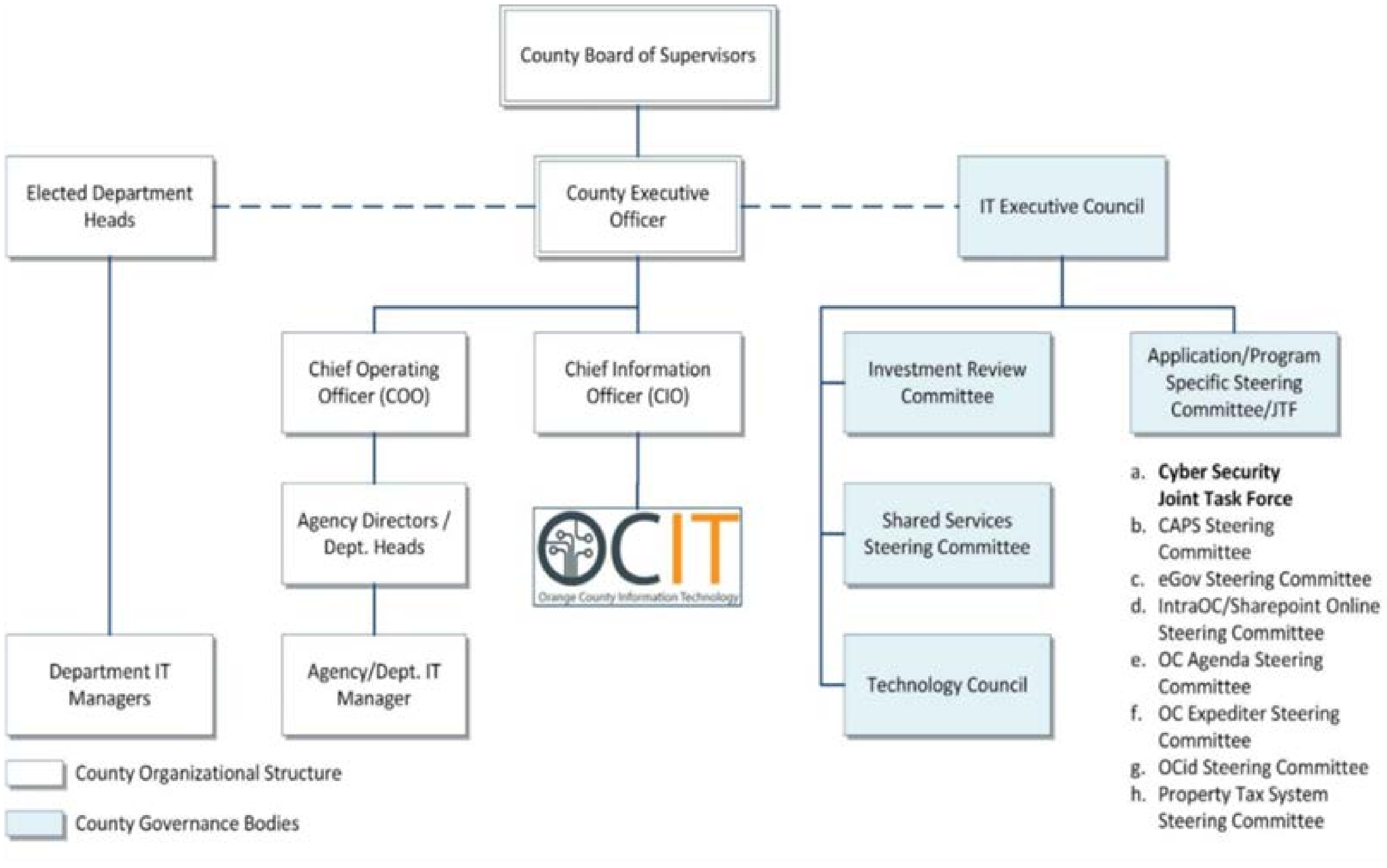
The following groups shall be notified via e-mail and/or in writing upon approval of the Manual and upon any subsequent revisions or amendments made to the original document:

- Board of Supervisors
- CEO
- CIO
- IT Executive Council
- Internal Audit

1.5 IT Governance Model

IT governance consists of leadership, stakeholder engagement, and collaboration processes that ensure that the County's IT investments support overall business strategies and policy objectives. IT governance facilitates general agreement on IT policies, resources, and architecture.

The IT Executive Council receives input from multiple committees, task forces, and working groups, including the CSJTF and Technology Council. Changes or updates to this policy may be proposed by any group. The CSJTF and Technology Council are responsible for researching and proposing IT guiding principles, standards, policies, and guidelines to the IT Executive Council. The CSJTF works collaboratively with the Technology Council to make recommendations to the IT Executive Council through the governance process. The Technology Council also advises the office of the CIO as appropriate. As needed, proposals will be forwarded to the IT Executive Council for review and submission to the CEO for approval.


County Board of Supervisors
Elected Department Heads
County Executive Officer
IT Executive Council
Chief Operating Officer (COO)
Chief Information Officer (CIO)
Investment Review Committee
Application/Program Specific Steering Committee/JTF
Agency Directors / Dept. Heads
OCIT
Orange County Information Technology
Shared Services Steering Committee
Department IT Managers
Agency/Dept. IT Manager
Technology Council
a. Cyber Security Joint Task Force
b. CAPS Steering Committee
c. eGov Steering Committee
d. IntraOC/Sharepoint Online Steering Committee
e. OC Agenda Steering Committee
f. OC Expediter Steering Committee
g. OCid Steering Committee
h. Property Tax System Steering Committee
County Organizational Structure
County Governance Bodies

2 Cybersecurity Program Roles and Responsibilities

The roles and responsibilities associated with implementation of the Cybersecurity Program include:

Chief Information Officer

- The Chief Information Officer (CIO) is overall responsible for the security of County data while it resides or flows on the County Enterprise Network. The CIO is the primary point of contact for the Chief Executive Officer (CEO) and Board of Supervisors for Information Technology and Cybersecurity.

Chief Information Security Officer

- The Chief Information Security Officer (CISO) is overall responsible for the County Cybersecurity Program (CSP).
- Oversees the creation, implementation, management and enforcement of the County CSP and cybersecurity policies, standards, and procedures.
- Ensures regular assessments and audits are conducted in order to validate compliance with County cybersecurity policies, standards, and procedures.
- Assists Departments with becoming and/or maintaining compliance with the requirements of applicable federal, state and local laws and regulations.
- Conducts periodic review of Departmental CSPs and provides feedback for the sustainment and/or improvement of cybersecurity plans, policies, standards, and procedures.
- Reports to the CIO on all Cybersecurity and Privacy Activities, reports to CEO as required.

Department Heads

- The Department Heads are responsible for determining the acceptable level of risk, as it pertains to the impact of cybersecurity on their respective department's lines of business including approval of Cybersecurity Policy Exemption Request forms (may **NOT** be delegated).
- The Department Heads may, in writing, appoint a member of their staff to function and carry out the duties of the Departmental Information Security Officer (DISO) and Custodian of Records.
- Overall responsible for the integrity of department computer infrastructure and systems.
- Overall responsible for application of technical safeguards of department computer infrastructure and systems except those departments participating in OCIT Shared Services.

Orange County Information Technology Shared Services

- Oversees information technology services for departments subscribed to the IT shared services.
- Coordinates with departments (subscribed to IT shared services) the delivery for information technology related initiatives and operational issues.
- Responsible for operation and maintenance of department computer infrastructure and systems for participating departments.
- Responsible for application of technical safeguards of department computer infrastructure and systems for participating departments.

Department Information Technology Manager

- The Department Information Technology Manager (IT Manager) is directly responsible for all Department Information Systems. The IT Manager is the primary point of contact for the Department Heads, Chief Information Officer (CIO) and Chief Information Security Officer (CISO).

Department Information Security Officer (DISO)

- Role is authorized by the Department Head and the following functions may be performed by an existing position (Does not require a new department position):

For departments using Shared Services:

- **Serves as liaison** between CISO, County Privacy Officer and Department for issues pertaining to cybersecurity and privacy.
- **Serves as liaison** between CISO, OCIT technical staff, and the Department for implementation of technical controls and remediation of technical findings from cybersecurity assessments, audits, and cybersecurity incidents.
- **Serves as liaison** between CISO, County Privacy Officer and Department to annually review and approve the Department's cybersecurity policies.
- **Serves as liaison** between CISO, OCIT technical staff, OCIT Business Relationship Management (BRM), and Department to annually review and test Business Continuity, Disaster Recovery, and Cyber Incident Response Plan (CIRP).
- **Serves as liaison** between CISO, OCIT BRM, and Department for communicating cybersecurity and privacy policy to staff and submitting cybersecurity exemption policy requests via the approved process.
- Works with CISO and County Privacy Officer to maintain confidential and accurate records related to Department's Cybersecurity and Privacy Incidents.

All other departments:

- **Serves as liaison** between CISO, County Privacy Officer and Department for issues pertaining to cybersecurity and privacy.
- Responsible for the Maintenance of departmental CSP, and ensures cybersecurity policies, processes and procedures must be at least as comprehensive but may be more stringent than the County's.
- **Serves as liaison** with technical staff for the implementation of technical controls and remediation of technical findings from cybersecurity assessments, audits and cybersecurity incidents.
- Annually reviews and approves the Department's cybersecurity policies.
- Conducts reviews and testing with the County CISO of Business Continuity, Disaster Recovery and Cyber Incident Response Plans (CIRP).
- Responsible for communicating this policy to their users and submitting cybersecurity exemption policy requests via the approved process.
- Maintains confidential and accurate records related to Cybersecurity and Privacy Incidents.

Department Custodian of Records

- Point of contact for department regarding PRA issues.
- Facilitates access to departmental records.
- For e-Discovery matters, works directly with the Enterprise e-Discovery Manager and refers all Security, HRS investigations back to the Enterprise e-Discovery Manager and follows the approved e-Discovery processes.
- Consults with County Counsel about the application of legal requirements for managing the department records, and applicable data retention policies and procedures.

- Maintains records as required by “Legal Hold” and data “Preservation” actions in conjunction with legal matters.
- Compiles the necessary data in response to Public Records Act (PRA) inquiries.
- Collaborates with the County Counsel for legal matters.
- Collaborates with CEO/HRS/County Counsel regarding redactions.
- Collaborates with the County Risk Management and County Counsel regarding claims for and against the County.
- Collaborates with the OCIT – Enterprise Security for collection and redaction of applicable County Data when responding to Public Records Act (PRA) inquiries.

CyberSecurity Joint Task Force (CSJTF)

- Serves as a joint advisory body to the IT Executive Council on all matters of cybersecurity policy and procedure development, implementation and enforcement.
- Conducts annual review of the County CSP and provide recommendations for changes.

County Cyber Resilience Manager

- Coordinates with departments to perform annual self-assessments based on Department of Homeland Security (DHS) Cyber Resilience Review.
- Assists departments with scheduling and preparation for third party cybersecurity audits.
- Provides cybersecurity assessment for departments in order to help remediate issues prior to audits and assist with remediation of findings post audit.
- Manages GRC platform to oversee plan of action and milestone tracking for remediation of identified gaps.
- Provides assistance with development of scopes for penetration testing, vulnerability scans and cybersecurity audits.
- Provide department support and coordinates for disaster recovery planning and testing.

County Privacy Officer

- Provides oversight, development, implementation and review of the County privacy programs.
- Provides oversight of the Data Loss Prevention policies and procedures.
- Oversees County Cybersecurity Awareness Training and HIPAA, PII, PHI, and other Privacy and Security trainings.
- Conducts HIPAA compliance reviews and ensures departments are in compliance with all applicable privacy regulations.
- Supports Contracts and Procurement to ensure appropriate privacy and security language is in place to protect and safeguard County data.
- Establishes reporting methods to detect privacy incident, conduct investigations, breach risk assessments and develop corrective action plans.
- Coordinates notification to state, federal and breach affected individuals and assist departments with regulatory privacy audits.

County e-Discovery/Public Records Act Manager

- Oversees the County’s IT Security e-Discovery program and acts as the in-house IT Security e-Discovery consultant for all departments.
- Conducts investigations and manages the production of Root Cause Analysis for cybersecurity incidents.

- Provides oversight and support coordination for e-Discovery services.
- Provides support for handling of digital evidence for Human Resource Services (HRS) investigations.
- Provides e-Discovery litigation support for various legal activities as required by County Counsel or Risk Management departments or their outside Counsels.
- Provides oversight of the vendor forensic services.
- Provides oral and written testimonies.
- Oversees and manages the IT Security processes for collection, processing and reviews of Public Records Acts requests and coordinates all work with:
  * Custodian of Records
  * County Counsel
  * Public Information Officers
  * Suppliers
  * Various IT teams
- “Public Records” may include any data relating to the conduct of the public's business prepared, owned, used, or retained by the County of Orange.

County Security Operations Service Delivery Manager

- Oversees OC Data Center (DC) Security Operations Center (SOC).
- Provides oversight of the Network Security Software and Appliances Policy.
- Provides support for the cyber incident identification, isolation, eradication, and remediation process.
- Coordinates with departments the delivery for security related initiatives and security operational issues.
- Provides support for security appliances and tools (HDLP, NDLP, IDS/IPS, firewalls, e-mail gateway, and web proxy services).
- Coordinates the County Disaster Recovery testing and implementation.

County Public Information Office (PIO)

- The County Public Information Office works in coordination with the CISO and County Privacy Officer on any proposed notification materials to the media.

Service Desk

- The Service Desk is responsible for opening tickets that are forwarded to the appropriate party for resolution.

County Counsel (CoCo)

- Provides consultation to the Cyber Incident Response Team as needed or applicable.
- Provides legal analysis or county counsel opinion as needed regarding local, State, Federal, and contractual obligations.

County Risk Manager

- Point of contact for Cyber Insurance Provider.
- Collaborates with affected system owner to report the financial value of compromised assets and information to the insurance provider.

County Data Center Manager

- Oversees County of Orange Data Center
- Coordinates with departments the delivery for information technology related initiatives and operational issues.

Human Resources Manager

- Point of contact for OCIT – Enterprise Security for electronic incidents involving County employees.

Vendors

- Comply with County and departmental policies, standards and procedures.

End Users

- Comply with County and departmental policies, standards and procedures.

3 Cybersecurity Program

3.1 Cybersecurity Program Overview

A strong cybersecurity position is achievable through the implementation, application and management of departmental cybersecurity programs (CSP). To maintain a strong cybersecurity position, it is essential for CSPs to include procedures and controls implemented within a department to secure data and information systems.

Each department is required to develop a departmental CSP. The procedures and controls included in the departmental CSP shall be determined by each department. The following sections describe the best practices of a CSP and provide a framework to establish a secure environment that safeguards the confidentiality, integrity and availability of the data and information systems used to manage the services provided by the County. **This document is intended to provide guidelines for departments to use in developing, implementing and maintaining an effective CSP; any changes or modifications to the guidelines should be discussed with OCIT.** Additionally, the departmental CSP should address any state, federal, regulatory, and contractual obligations that impact the department's data and information systems (refer to *Appendix K: Listing of State and Federal Laws and Regulations*).

3.2 Cybersecurity Program Domains

The CSP defines the County's capacities and capabilities in performing, planning, managing, measuring, and cybersecurity practices and behaviors through the following ten domains which are consistent with the Department of Homeland Security's Cyber Resilience Review (refer to the links listed in Section 8: References):

ASSET MANAGEMENT

CONTROLS MANAGEMENT

CONFIGURATION AND CHANGE MANAGEMENT

VULNERABILITY MANAGEMENT

INCIDENT MANAGEMENT

SERVICE CONTINUITY MANAGEMENT

RISK MANAGEMENT

EXTERNAL DEPENDENCY MANAGEMENT

TRAINING AND AWARENESS

SITUATIONAL AWARENESS

The above-mentioned domains (detailed in sections 3.2.1 through 3.2.10) are the minimum components of a CSP. To support these domains, tools and plans are necessary and developed. They also support the application of security controls, data ownership responsibilities, and maintenance of the security infrastructure. The development of the departmental CSP including these domains is the responsibility of each department. Refer to Section 2: *Roles and Responsibilities* of this Manual for more information on individual roles.

3.2.1 Asset Management

Asset management establishes an organization's inventory of fixed and controlled assets and defines how these assets are managed during their lifecycle to ensure sustained productivity in support of the organization's critical services. The CSP shall define four broad categories of assets:

people, information, technology, and facilities. An event that disrupts an asset can inhibit the organization from achieving its mission. An asset management program helps identify appropriate strategies that will allow the assets to maintain productivity during disruptive events.

The Asset Management domain focuses on the processes by which an organization:

- Plan for Asset Management—Highlights the elements necessary for an effective asset management plan
- Identify the Assets—Presents a process for identifying assets based on asset type (People, Information, Technology, Facilities)
- Document the Assets—Provides an approach for documenting assets
- Manage the Assets—Outlines a process for managing assets within the organization

The CSP strives to achieve and maintain appropriate protection of IT assets. Loss of accountability of IT assets could result in a compromise or breach of IT systems and/or a compromise or breach of sensitive or privacy data. Processes shall be in place to address the following:

- Inventory and tracking of physical IT equipment to include, but not limited to, the following: (1) Desktop computers, (2) Laptop Computers, (3) Tablets (iPads and Android devices), (4) Mobile Phones (basic cell phones), (5) Smart Phones (iPhones, Blackberry, Windows Phones and Android Phones), (6) Servers, (7) Storage devices, (8) Network switches, (9) Routers, (10) Firewalls, (11) Security Appliances, (12) Internet of Things (IoT) devices, (13) Printers, (14) Scanners, (15) Kiosks and Thin clients, (16) Mainframe Hardware, (17) VoIP Phones, or any other device that connects to the County networks and/or stores or processes county data.
- Disposition of physical IT equipment to include, but not limited to, the following: (1) Location, (2) Operational status (in use or not online), (3) Custodian of Equipment, (4) Transfer logs, (5) Surplus, (6) Deliberate destruction of equipment (for security purposes such as hard drives, tablets, etc.), (7) Loss of equipment (Destroyed accidentally, stolen or simply lost).

Refer to *Appendix A – Asset Management Controls* for additional guidance and controls related to asset management process.

3.2.2 Controls Management

The Controls Management domain focuses on the processes by which an organization plans, defines, analyzes, and assesses the controls that are implemented internally. This process helps the organization ensure the controls management objectives are satisfied.

This domain focuses on the resilience controls that allow an organization to operate during a time of stress. These resilience controls are implemented in the organization at all levels and require various levels of management and staff to plan, define, analyze, and assess. The high-level outline below highlights the main areas of this domain:

- Plan for Controls Management—Highlights the elements necessary for an effective controls management plan;
- Define Controls—Presents a process for defining controls based on identified objectives;

- Analyze and Deploy Controls—Provides a step-by-step approach for controls analysis and deployment; and
- Assess Controls—Outlines a process for scheduling, scoping, and performing assessments of controls.

Refer to *Appendix B – Controls Management Controls* for additional guidance and controls related to controls management process.

3.2.3 Configuration & Change Management

Configuration and Change Management (CCM) is the process of maintaining the integrity of hardware, software, firmware, and documentation related to the configuration and change management process. CCM is a continuous process of controlling and approving changes to information or technology assets or related infrastructure that support the critical services of an organization. This process includes the addition of new assets, changes to assets, and the elimination of assets.

Cybersecurity is an integral component to information systems from the onset of the project or acquisition through implementation of:

- Application and system security
- Configuration management
- Change control procedures
- Encryption and key management
- Software maintenance, including but not limited to, upgrades, antivirus, patching and malware detection response systems

As the complexity of information systems increases, the complexity of the processes used to create these systems also increases, as does the probability of accidental errors in configuration. The impact of these errors puts data and systems that may be critical to business operations at significant risk of failure that could cause the organization to lose business, suffer damage to its reputation, or close completely. Having a CCM process to protect against these risks is vital to the overall security posture of the organization. The four phases of the CCM process:

- Create a Configuration and Change Management Plan—Details the process of creating a configuration and change management plan and identifies details that an organization should consider when developing its plan.
- Identify Configuration Items—Details the process of identifying assets that support critical services and will be configured and managed using this process.
- Implement and Control Configuration Changes—Details the process by which changes are approved, executed, and brought to closure.
- Monitor Configuration Changes—Details the process for assessing whether changes have occurred and procedures for addressing unauthorized changes.

Refer to *Appendix C – Configuration and Change Management Controls* for additional guidance and controls related to configuration and change management process.

3.2.4 Vulnerability Management

The Vulnerability Management domain focuses on the process by which organizations identify, analyze, and manage vulnerabilities in a critical service's operating environment. The vulnerability management process is divided into four phases:

- Define a Vulnerability Analysis and Resolution Strategy—Provides an approach for determining the contents of an appropriate strategy.
- Develop a Plan for Vulnerability Management—Outlines a plan creation process and identifies issues and considerations to help ensure that the plan addresses the organization's needs.
- Implement the Vulnerability Analysis and Resolution Capability—Outlines an approach for putting your plan, team, and tools into operation in support of the organization.
- Assess and Improve the Capability—Outlines the process for improving your organization's ability to discover and resolve those vulnerabilities most pertinent to your organization and adjust your plan accordingly.

Refer to *Appendix D – Vulnerability Management Controls* for additional guidance and controls related to asset management process.

3.2.5 Incident Management

The process of detecting, analyzing, responding to, and improving from disruptive events is known as incident management. The goal of incident management is to mitigate the impact of a disruptive event. To accomplish this goal, an organization establishes the following processes:

- detect and identify events
- triage and analyze events to determine whether an incident is underway
- respond and recover from an incident
- improve the organization's capabilities for responding to a future incident

The incident management process involves:

- Create an Incident Management Plan—Outlines a plan creation process and identifies issues and considerations to help ensure that the plan addresses the organization's needs.
- Test the Incident Management Plan—Outlines the process and considerations for testing an incident management plan.
- Improve the Incident Management Plan—Outlines the process and considerations for improving your incident management plan so that it continues to address your organization's needs.

This domain defines management controls for addressing cyber incidents. The controls provide a consistent and effective approach to Cyber Incident Response aligned with Orange County's Cyber Incident Response Plan, to include:

- Collection of evidence related to the cyber incident as appropriate
- Reporting procedures including any and all statutory reporting requirements
- Incident remediation
- Minimum logging procedures
- Annual testing of the plan

Refer to *Appendix E – Incident Management Controls* for additional guidance and controls related to incident management process.

3.2.6 Service Continuity Management

Service continuity planning is one of the more important aspects of resilience management because it provides a process for preparing for and responding to disruptive events, whether natural or man-made. Operational disruptions may occur regularly and can scale from so small that the impact is essentially negligible to so large that they could prevent an organization from achieving its mission. Services that are most important to an organization's ability to meet its mission are considered essential and are focused on first when responding to disruptions. The process of identifying and prioritizing services and the assets that support them is foundational to service continuity.

Service continuity planning provides the organization with predefined procedures for sustaining essential operations in varying adverse conditions, from minor interruptions to large-scale incidents. For example, a power interruption or failure of an IT component may necessitate manual workaround procedures during repairs. A data center outage or loss of a business or facility housing essential services may require the organization to recover business or IT operations at an alternate location.

The process of assessing, prioritizing, planning and responding to, and improving plans to address disruptive events is known as service continuity. The goal of service continuity is to mitigate the impact of disruptive events by utilizing tested or exercised plans that facilitate predictable and consistent continuity of essential services. To accomplish this goal, an organization establishes processes that:

- Establish and Maintain a Service Continuity Program—Outlines a program creation process and identifies issues and considerations to help ensure that the program addresses the organization's needs.
- Perform Service Continuity Planning—Provides a step-by-step approach to developing continuity plans following the approach developed.
- Validate and Exercise Service Continuity Plans—Outlines the process for ensuring that the organization's service continuity plans meet standards set by the organization; outlines the process of exercising service continuity plans.
- Improve Service Continuity—Outlines the process and considerations for improving the service continuity program as well as plans.

This domain defines requirements to document, implement and annually test plans, including the testing of all appropriate cybersecurity provisions, to minimize impact to systems or processes from the effects of major failures of information systems or disasters via adoption and annual testing of:

- Business Continuity Plan
- Disaster Recovery Plan
- Cyber Incident Response Plan

Refer to *Appendix F – Service Continuity Management Controls* for additional guidance and controls related to service continuity management process.

3.2.7 Risk Management

The risk management domain focuses on the processes by which an organization identifies, analyzes, and mitigates risks in order to affect the probability of their realization and/or the impact of a disruption. It is a foundational activity for any organization and is practiced at all levels of the organization, from the executives down to individuals within business units. Organizations must manage many different types of risk to remain effective and achieve their objectives. The pervasiveness of the threats to information and the dynamics of today's global operational environment require ongoing collaboration facilitated by two-way internal and external communication.

To effectively manage operational risk, organizations should establish processes to:

- identify risks to which the organization is exposed
- analyze risks and determine appropriate risk disposition
- control risks to reduce probability of occurrence and/or minimize impact
- monitor risks and responses to risks and improve the organization's capabilities for managing current and future risks

The risk management process involves:

- Create a Risk Management Plan—Outlines a strategy and plan creation process and identifies issues and considerations to help ensure that the plan addresses the organization's risk management needs.
- Implement the Risk Plan—Outlines the process for ensuring that the organization's risk management plan is implemented and meets the standards set by the organization.
- Monitor and Improve Operational Risk Management—Outlines the process and considerations for keeping the risk management process resilient and robust.
- Risk-Based Approach

Refer to *Appendix G – Risk Management Controls* for additional guidance and controls related to risk management process.

3.2.8 External Dependencies Management

In today's technology and business environment, organizations often rely on outside entities, including technology vendors, suppliers of raw materials, shared public infrastructure, and other public services that support the organization. External dependencies management (EDM) focuses on establishing an appropriate level of controls to manage the risks that originate from or are related to the organization's dependence on these external entities. The purpose of EDM is to ensure the protection and sustainment of services and assets that are dependent on the actions of external entities.

Identifying, prioritizing, and managing relationships with external entities over their entire lifecycle are foundational activities for the development of effective risk mitigation and disposition strategies. To effectively manage external dependencies, organizations should establish:

- a strategy and basic plan for EDM
- key processes for identifying, prioritizing, monitoring, and tracking external dependencies
- guidance and procedures on the formation of relationships with external entities
- an approach for managing and governing existing external entity relationships
- ongoing oversight, reporting, and correction of external entity performance
- an approach for improving the organization's EDM processes and program

Like many key resilience practices, EDM should be thought of as a planned, continuous process. In the case of EDM in particular, many organizations may have only ad hoc or incomplete processes around forming new relationships with external entities or around managing existing relationships.

It is also not unusual for particular organizations to have detailed procedures around the formation of new relationships, but for the ongoing management of relationships to run according to a substantially different set of objectives or standards. Effective EDM requires standard, planned guidance across the entire lifecycle of external entity relationships and continuous monitoring and improvement of the approach.

The primary phases of the EDM process are:

- Plan for External Dependencies Management—Outlines a strategy and plan creation process and identifies issues and considerations to help ensure that the plan addresses the organization’s external dependencies management needs.
- Implement the External Dependencies Management Plan—Outlines the process for ensuring that the organization’s external dependencies management plan is implemented and meets the standards set by the organization.
- Monitor and Improve External Dependencies Management—Outlines the process and considerations for improving and strengthening the external dependencies management process.

Refer to *Appendix H – External Dependencies Management Controls* for additional guidance and controls related to external dependencies management process.

3.2.9 Training and Awareness

Training and awareness focuses on the processes by which an organization plans, identifies needs for, conducts, and improves training and awareness to ensure the organization’s operational cyber resilience requirements and goals are known and used.

The following sections detail each of the steps in the training and awareness process:

- Plan for Training and Awareness—Highlights the elements necessary for an effective training and awareness plan.
- Assess Training and Awareness Needs—Presents an approach for identifying cybersecurity-related skills needed for specific roles (administrators, technicians, etc.) and cybersecurity awareness needs for staff throughout the organization.
- Conduct Training and Awareness Activities—Outlines a process that defines the steps necessary to manage, develop, schedule, and conduct training and awareness activities.
- Improve Training and Awareness Capability—Provides an approach for evaluating and improving training and awareness capability.

Refer to *Appendix I – Training and Awareness Controls* for additional guidance and controls related to training and awareness process.

3.2.10 Situational Awareness

Situational awareness provides an organization an understanding of its critical service’s operating environment and the environment’s impact on the operation of the critical service. This understanding provides stakeholders with a sufficiently accurate and up-to-date understanding of the past, current, and projected future state of a critical service and supports effective decision making in the context of a common operating environment. This includes understanding the assets and other services that affect or depend on the critical service. The representation or picture of the state of a critical service (including the condition of its supporting assets, the performance of its high-value physical and cyber processes, and events detected and responded to by its physical and cybersecurity safeguards) is presented to stakeholders in the context of the threat environment (internal and external) and the resulting risks to the critical service's mission.

The situational awareness process establishes a *common operating picture* (COP) by collecting, fusing, and analyzing data to support automated or human decisions about appropriate actions to prevent disruption of a critical service or to restore the service to proper function. This COP is shared through timely communication and presentation of the results of the data analysis to appropriate decision makers (people or machines) in a form that aids human comprehension (e.g., using data visualization techniques, appropriate use of alarms) and allows operators or other personnel to quickly grasp the key elements needed for good decision making.

The COP should be accurate and actionable (appropriate for supporting good decisions and actions). However, different members of an organization likely need different, and not necessarily complete, views of the operational environment. Depending on how it is presented, a complete picture could present too much information and overload a human decision maker. Operators should not be presented with a massive data dump; rather, operators should see only what's important, which is determined by the risk strategy and overall risk picture.

Communication between situational awareness and other organizational processes is bi-directional. Other processes report information, such as vulnerabilities, incidents, and risk management decisions, to the situational awareness process. At the same time, the situational awareness process contributes the information, or improves its quantity or quality, needed by other processes that inform decision making or appropriate actions.

Communication among processes relies on their linkages. These linkages can be simple, such as reporting of suspicious events to the incident response team. They can also be complex, such as asset and controls management processes that include an intrusion detection system (IDS) that monitors assets and services deemed important by the risk management process and alerts those who can take mitigating steps.

The high-level outline below highlights the four phases of this process:

- Plan for Situational Awareness—Highlights the elements necessary for an effective situational awareness plan.
- Collect and Analyze Situational Awareness Data—Presents an approach for identifying and managing the requirements for situational awareness data collection and analysis, including recommended categories of information to be monitored to assure organizational resilience and an approach for analyzing situational awareness information.
- Communicate Information Needed to Make Appropriate Decisions—Outlines a process that defines steps necessary to manage the communication of information to appropriate staff, enabling them to make informed decisions and identify follow-up actions.
- Improve Situational Awareness Processes and Technology—Provides an approach for reviewing and improving the organization's situational awareness capability.

Threat intelligence is often presented in the form of Indicators of Compromise (IoCs) or threat feeds. Threat intelligence requires organizations to understand themselves first and then understand the adversary. The County may use information from a variety of intelligence sources to identify and mitigate risks in the current cyberspace. Departments are free to either procure their own Cyber Intelligence services and advisories or they may subscribe to the OCIT provided intelligence services. Intelligence services, at a minimum, must perform the following:

Impact of Cyber Threats Assessment

The impact of cyber threats is evaluated against the likelihood and possible harm of a potential threat. Analysis includes:

- Probability of each threat occurring.
- Cost if each threat were to actually occur. Costs should be interpreted broadly to include money, resources, time, and loss of reputation among others.
- Cost, in money or effort, to prepare preemptive mitigation of probable cyber threats.

Refer to *Appendix J – Situational Awareness Controls* for additional guidance and controls related to situational awareness process.

4 Administrative Controls

4.1 County Cybersecurity Policy

Placeholder for link to County Cybersecurity Policy (being updated).

4.2 County IT Usage Policy

Placeholder for link to County IT Usage Policy (being updated).

5 Technical Controls

The controls described in this section are provided as best practices and are intended to assist departments with developing their departmental IT security policies. Only those items included in the County IT Security Policy are required to be implemented by the departments.

5.1 Asset Management

Devices

5.1.1. Deploy automated asset inventory discovery tools (both passive and active).

5.1.2. Deploy both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic and use it to maintain an accurate asset inventory of devices connected to the County's public and private network(s).

5.1.3. Deploy Dynamic Host Configuration Protocol (DHCP) Server logging, and utilize a system to improve the asset inventory and help detect unknown systems through this DHCP information.

5.1.4. All equipment acquisitions shall be updated in the asset inventory as new, approved devices are connected to the network.

5.1.5. A robust change control process shall be used to validate and approve all new devices.

5.1.6. Maintain an asset inventory of all devices connected to the network and the network devices themselves recording at least: the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device, type of device (mobile, personal, etc.).

5.1.7. The inventory shall include every device that has an Internet Protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc.

5.1.8. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store, process or transmit data shall be identified, regardless of whether or not they are attached to the organization's network.

Notes: It seems reasonable to assert that such accounting shall be as good as the last active contact made with the asset. There may be some creative ways to understand the 'last known contact' beyond the obvious 'connected to network' case. It might be reasonable to interrogate a mail server for the last time that asset retrieved mail, as one example.

5.1.9. Make sure the asset inventory database is properly protected and a copy stored in a secure location.

5.1.10. In addition to an inventory of hardware, organizations shall develop an inventory of information assets that identifies their “critical” information.

5.1.11. Information asset inventory shall map critical information to the hardware assets (including servers, workstations, and laptops) on which it is stored.

5.1.12. A department and individual responsible for each information asset shall be identified, recorded, and tracked.

5.1.13. Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network.

5.1.14. 802.1x shall be tied into the inventory data to determine authorized vs. unauthorized systems.

Notes: The Asset Inventory System needs to be integrated with the port-based NAC controls the enterprise has in place. TCG formats and protocols do not speak Asset Identification, but they may speak something else that can be mapped to the Asset Identification specification. Additionally, it seems warranted that the access control lists managed by a TCG Policy Decision Point shall be something understood by the Asset Inventory System. This is another point of integration that would be best performed outside of enterprises, but that will likely be performed inside enterprises.

5.1.15. Utilize client certificates to validate and authenticate systems prior to connecting to the private network. (County Policy for external facing devices only)

5.1.16. Organizations shall stand up and manage a Certificate Authority within their organization.

Notes: Installing and managing a Public (to your organization) Key Infrastructure (PKI) is not necessarily a piece of cake. An alternative is the Certificate Enrollment Process. It seems the most critical overall (assuming your key generation and lifecycle are under control for your root). Some platform families make extensive use of application-specific PKI.

5.1.17. Organizations shall first establish information/asset owners, deciding and documenting which organizations and individuals are responsible for each component of a business process that includes information, software, and hardware.

5.1.18. In particular, when organizations acquire new systems, they record the owner and features of each new asset, including its network interface media access control (MAC) address and location. This mapping of asset attributes and owner-to-MAC address can be stored in a free or commercial database management system.

5.1.19. Use tools to pull information from network assets such as switches and routers regarding the machines connected to the network.

5.1.20. Using securely authenticated and encrypted network management protocols, tools can retrieve MAC addresses and other information from network devices that can be reconciled with the organization’s asset inventory of servers, workstations, laptops, and other devices.

5.1.21. Once MAC addresses are confirmed, switches shall implement 802.1x and NAC to only allow authorized systems that are properly configured to connect to the network.

5.1.22. Effective organizations configure free or commercial network scanning tools to perform network sweeps on a regular basis, sending a variety of different packet types to identify devices connected to the network.

Notes: Before such scanning can take place, organizations shall verify that they have adequate bandwidth for such periodic scans by consulting load history and capacities for their networks.

5.1.23. In addition to active scanning tools that sweep the network, other asset identification tools passively listen on network interfaces looking for devices to announce their presence by sending traffic.

5.1.24. Such passive tools can be connected to switch span ports at critical places in the network to view all data flowing through such switches, maximizing the chance of identifying systems communicating through those switches.

5.1.25. Whether physical or virtual, each machine using an IP address shall be included in an organization’s asset inventory.

5.1.26. The system shall be capable of identifying any new unauthorized devices that are connected to the network.

5.1.27. Alerting or sending e-mail notification to a list of enterprise administrative personnel within 1 hour.

5.1.28. The system shall automatically isolate the unauthorized system from the network within one hour of the initial alert

5.1.29. Send a follow-up alert or e-mail notification when isolation is achieved.

5.1.30. Every 24 hours after that point, the system shall alert or send e-mail about the status of the system until the unauthorized system has been removed from the network.

5.1.31. The asset inventory database and alerting system shall be able to identify the location, department, and other details of where authorized and unauthorized devices are plugged into the network.

Standard Naming Convention

5.1.32. Assets shall be named using the following standard naming convention as devices are serviced or purchased:

- Organization (see Organization table)
- Program (option for departments)
- Location (see Location table)
- Acquisition Year (optional)

- Type (see Type table)
- Unique Number (e.g., Asset Tag #, Serial #, etc.)

Example: ITXXSA2018LT123456

- OCIT (IT)
- None (XX)
- St Andrews (SA)
- 2018
- Laptop (LT)
- 123456

Software

5.1.33. Devise a list of authorized software that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses.

5.1.34. This list shall be tied to file integrity checking software to validate that the software has not be modified.

5.1.35. Perform regular scanning and generate alerts when unapproved software is installed on a computer.

Notes: "Scanning" involves three steps: 1) harvesting information from your computing devices, 2) comparing the information you have harvested against your whitelist of authorized software, and 3) generating an alert when an unauthorized piece of software is discovered.

5.1.36. A strict change control process shall also be implemented to control any changes or installation of software to production systems on the network.

5.1.37. Deploy application white listing technology that allows systems to run only approved software and prevents execution of all other software on the system.

5.1.38. Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops.

5.1.39. The software inventory system shall track the version of the underlying operating system as well as the applications installed on it.

5.1.40. Furthermore, the tool shall record not only the type of software installed on each system, but also its version number and patch level.

5.1.41. The software inventory shall be tied to vulnerability reporting/threat intelligence services to fix vulnerable software proactively.

5.1.42. The software inventory systems shall be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.

5.1.43. The software inventory tool shall also monitor for unauthorized software installed on each machine. This includes legitimate system administration software installed on inappropriate systems where there is no business need for it.

5.1.44. Dangerous file types (e.g., exe, zip, msi, etc.) shall be closely monitored and/or blocked.

5.1.45. Software inventory and application white listing shall also be deployed on all mobile devices that are utilized across the organization.

5.1.46. Virtual machines and/or air-gapped systems shall also be used to isolate and run applications that are required but based on higher risk and that shall not be installed within a networked environment.

5.1.47. Configure client workstations with non-persistent virtualized operating environments that can be quickly and easily restored to a trusted snapshot on a periodic basis.

5.1.48. Deploy software that only provides signed software ID tags (the ISO 19770 Software ID tags managed by TagVault.org).

5.1.49. The software inventory tools shall provide an inventory check of hundreds of common applications used in enterprises, pulling information about the patch level of each installed program to ensure that it is the latest version and leveraging standardized application names, such as those found in the common platform enumeration specification.

Information

5.1.50. Establish a multi-level data identification/classification scheme (e.g., a three- or four-tiered scheme with data separated into categories based on the impact of exposure of the data).

Access Control

Access controls are measures for ensuring that only users with the proper need and authority can access the system and perform authorized functions on the systems. Applicable organizations' management and staff shall understand their responsibilities relative to access control.

Access Control Rules

5.1.51. Access control shall start by denying access to everything, and then explicitly granting access according to the "need to know" principle. County employees shall be granted access to information or information assets necessary to carry out their responsibilities.

5.1.52. Access to information and information assets shall be based on the principle of "least privilege," that is, grant no user greater access privileges to the information or assets than their responsibilities demand.

5.1.53. The "least privilege" principle shall also be applied to users' modes of access, such as whether the individual is granted "read or write" privileges.

5.1.54. Track or document which individuals are authorized to issue user IDs to employees and restrict authority to issue user IDs to those identified individuals.

5.1.55. Track or document the access control level privileges that may be granted and restrict individuals' access to authorized levels.

5.1.56. Track or document the access levels granted to each registered employee.

5.1.57. Conduct regular reviews of the registered employees' access level privileges.

5.1.58. Provide procedures to disable user accounts upon termination of employment or contractual obligation, and procedures to modify access privileges upon change in job responsibilities.

5.1.59. Employees shall be assigned only the access privileges needed for their job.

5.1.60. For any system that processes or stores sensitive (as defined by County Policy) information, password security will extend to the functional screen level and limit the user's capability to view and/or update those screens.

5.1.61. Each user will have a unique user account. Accounts shall NOT be shared at any time.

5.1.62. Employees shall log off or activate password-protected mechanisms (e.g., password-protected screensavers) before leaving the immediate vicinity of systems whenever possible.

Media Protection and Sanitation

5.1.63. Departments shall establish procedures and take the following actions to ensure that media is protected from unauthorized access, disclosure, modification, destruction or loss:

5.1.64. Restrict access to all media to authorized individuals with processes and/or mechanisms for authentication and authorization in accordance with *Section on Access Control*.

5.1.65. Physically control and securely store all media within controlled or normal work areas and protect from physical and environmental hazards. This includes but is not limited to employee desks or other local and remote work areas. Storage areas with significant volumes of media shall employ automated mechanisms to restrict and audit access.

5.1.66. Maintain confidentiality and acceptable use statements for system users in accordance with *County IT Usage Policy*.

5.1.67. Classify media in accordance with County Policy, commensurate with the highest level of information processed on the system with which it is used.

5.1.68. Mark removable or portable media containing sensitive (as defined by County Policy) material as "CONFIDENTIAL" to ensure proper handling and storage.

5.1.69. Protect and control media when traveling outside of normal work areas, and restrict the activities associated with the transport of such media to authorized personnel.

5.1.70. Employ the use of encryption in accordance with *Section on Encryption* when transporting digital media that contain County information.

5.1.71. Remove and/or sanitize digital media, where applicable, prior to sending off-site for maintenance.

5.1.72. Document activities associated with the transport of media containing County information with the use of logs or other tracking mechanisms.

5.1.73. Implement use of inventory logs, control numbers or other record-keeping methods in addition to appropriate physical protection for media containing sensitive (as defined by County Policy) data, which requires strict access accountability and/or chain-of-custody verification (including media sent off-site for maintenance). These logs shall be archived and made available for a period in compliance with County Records Management Policy.

5.1.74. Ensure departmental Custodians of Record are advised of security requirements and/or data sharing agreements to establish procedures for compliance with those requirements.

5.1.75. Permit only authorized digital media to process, access, and store County information.

5.1.76. Protect any media containing County information until the media are sanitized in accordance with National Security Agency (NSA) standards (for example, purging or destroying) when no longer needed or required.

5.1.77. Restrict reuse of digital media used for backup and/or data storage of County information only to the department's data.

5.1.78. Require offsite facilities used to store paper documents or digital media comply with County media protection and handling requirements and implement the same security provisions with that of the applicable organization's security requirements.

5.1.79. Sanitization methods for media containing County information shall be in accordance with NSA standards (for example, clearing, purging, or destroying).

5.1.80. Acquisitions for equipment intended for the use of processing or storing County information that include vendor return options for replacement or repair (such as off-site repair or maintenance) shall include provisions within the purchase agreement or documentation to allow destruction of all information and/or media prior to return for replacement or repair.

5.1.81. All storage media (magnetic, optical, electrical, or other) subject to vendor return agreements (such as but not limited to lease, warranty, rebate/refund etc.) shall have a method to appropriately sanitize the media of all residual data, using state- and federally-required methods prior to returning to vendor. Refer to *Section on Media Protection and Sanitation*.

5.1.82. All contracts or agreements for vendor-provided services for sanitation or disposal of media containing County information shall include provisions for a County employee to witness the media sanitation.

5.1.83. Prior to surplus, media that is obsolete or no longer usable shall either be purged or physically destroyed to ensure residual data cannot be recovered or reconstructed. Physical destruction methods include disintegration, incineration, pulverizing, or shredding. Refer to *Section on Media Protection and Sanitation*.

5.1.84. Sanitization procedures and equipment shall be periodically tested, where applicable, to verify correct performance.

5.1.85. Hardcopy documents, such as computer printouts, notes, work papers, etc., shall be destroyed using methods such as incineration, mulching, pulping, disintegration, or shredding. Hand-tearing or burying County information in landfills is an unacceptable method of disposal.

5.1.86. Sanitization of digital media or electronic surplus property containing sensitive (as defined by County Policy) data shall be witnessed by an applicable organization's employee, documented, and certified in writing. Certification records shall include information to identify media that was sanitized/destroyed, such as, property tag numbers, serial numbers and manufacturer, date of sanitization, sanitization method (clear, purge, destroy) and final disposition (vendor return, resale, donation, etc.) Certification records for media containing sensitive (as defined by County Policy) data shall be retained and made available per County Records Management Policy.

5.1.87. Prior to re-deployment, surplus, donation, disposal or destruction of equipment containing storage media, media shall be appropriately cleansed to prevent unauthorized exposure of data. NIST standards shall be followed for appropriate levels of storage media cleansing.

5.1.88. Disposal of equipment shall be done in accordance with all applicable County, state or federal surplus property and environmental disposal laws, regulations, or policies.

5.2 Control Management

Physical Security

5.2.1. All County departments that house information processing facilities are responsible for implementing procedures to follow the physical and environmental security policy, including identifying the perimeter of the facility and performing a risk analysis to assess its physical security.

5.2.2. All County employees, contractors, vendors, and customers are required to adhere to the physical and environmental security policies established by the authorized Department.

5.2.3. Procedures and facility hardening measures shall be adopted to prevent attempts at and detection of unauthorized access or damage to facilities that contain County information systems and/or processing facilities.

5.2.4. Restricted areas within facilities that house sensitive (as defined by County Policy) County information systems will, at a minimum, utilize physical access controls designed to permit access by authorized personnel only.

5.2.5. Physical protection measures against damage from external and environmental threats shall be implemented by all departments as appropriate.

5.2.6. Access to any office, computer room, or work area that contains sensitive (as defined by County Policy) information shall be physically restricted from unauthorized access.

5.2.7. Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. An example of this would be separating the two areas by a badge-only accessible door.

5.2.8. Continuity of power shall be provided to maintain the availability of critical equipment and information systems.

5.2.9. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. Different, yet appropriate, methods shall be utilized for internal and external cabling.

5.2.10. Equipment shall be properly maintained to ensure its continued availability and integrity.

5.2.11. Unless approved by County management, no County computer equipment shall be removed from the premises.

5.2.12. All shared IT infrastructure by more than one Department shall meet countywide security policy for facility standards, availability, access, data, and & network security.

Segregation of Duties

5.2.13. Segregation of duties shall be required to reduce the risk of accidental or deliberate system misuse. In small departmental IT functions in which separation of duties is difficult to achieve, OCIT - Enterprise Security approval and other compensatory controls shall be applied including implementation of additional controls including, but not limited to, activity monitoring, audit trails, and close management supervision. In all cases, the periodic security audits shall remain independent and shall be segregated from the security function.

Secure Network Configuration and Segmentation

5.2.14. The network shall be designed using a minimum of a three-tier architecture (demilitarized zone, middleware, and private network).

Notes: Can we justify the additional layering with any real-world data. For example, the Internet connects to the router, the router connects to the firewall, the firewall connects to everything internal. The DMZ would be the router-to-firewall portion of the topology, and may contain no hosts at all.

5.2.15. Any system accessible from the Internet shall be on the demilitarized zone (DMZ), but DMZ systems shall not store sensitive (as defined by County Policy) data.

5.2.16. Any system with sensitive (as defined by County Policy) data shall be 'permanently stored' behind the DMZ and served through the DMZ to properly authenticated entities over properly secured communication channels or shall reside on the private network and not be directly accessible from the Internet.

5.2.17. Any server that is visible from the Internet or an untrusted network shall be verified, and if it is not required for business purposes, it shall be moved to an internal Virtual Local Area Network (VLAN) and given a private address.

5.2.18. DMZ systems shall communicate with private network systems through an application proxy residing on the middleware tier.

5.2.19. To support rapid response and shunning of detected attacks, the network architecture and the systems that make it up shall be engineered for rapid deployment of new access control lists, rules, signatures, blocks, black holes, and other defensive measures.

5.2.20. DNS shall be deployed in a hierarchical, structured fashion, with all internal network client machines configured to send requests to intranet DNS servers, not to DNS servers located on the Internet.

5.2.21. Internal DNS servers shall be configured to forward requests they cannot resolve to DNS servers located on a protected DMZ.

Notes: Forward requests up the appropriate chain – you do not want unresolved DNS queries going directly from the sensitive (as defined by County Policy) tier to the Internet.

5.2.22. The DNS servers in the DMZ shall be the only DNS servers allowed to send requests (query service provider DNS servers) to the Internet. Additionally, such communications shall be performed over a secure channel.

5.2.23. VLAN1 shall not be used because it is the default VLAN for switches.

5.2.24. Segment (e.g., VLANs) the enterprise network into multiple, separate trust zones (based on trust levels of the information stored/transmitted) to provide more granular control of system access and additional intranet boundary defenses. Whenever information flows over a network of lower trust level, the information shall be encrypted.

Notes: This requires that you understand your business and its operational needs and habits. It does not make any sense to segment your networks if the organizational processes will just end up transiting those different ‘trust zones’ to get things done. Proper segmentation can simplify your compliance regime (required for PCI).

5.2.25. Create separate VLANs for BYOD (bring your own device) systems or other untrusted devices.

5.2.26. The network infrastructure shall be managed across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

5.2.27. Wireless access points shall never be directly connected to the private network. They shall either be placed behind a firewall or put on a separate VLAN so all traffic can be examined and filtered.

Perimeter Defense

5.2.28. Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (white lists).

Notes: Find a service that updates black lists and use it. If you actually know the communication patterns required throughout your organization well enough, then white lists are the way to go. Ensure that you control IP address changes otherwise using a white list could just be another way in.

5.2.29. Tests can be periodically carried out by sending packets from bogon source IP addresses (unrouteable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters.

Lists of bogon addresses are publicly available on the Internet from various sources (http://www.team-cymru.org/Services/Bogons/), and indicate a series of IP addresses that shall not be used for legitimate traffic traversing the Internet.

Notes: You are going to want to manage this blacklist in one location and propagate that list throughout your infrastructure.

5.2.30. On DMZ networks, monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) shall be configured to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border.

5.2.31. This traffic shall be sent to a properly configured Security Information and Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.

5.2.32. To lower the chance of spoofed e-mail messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.

5.2.33. Deploy network-based Intrusion Detection System (IDS) sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.

OR: Use network IDS especially in externally facing networks such as the DMZ. Everything else seems to make this overly prescriptive.

5.2.34. Design and implement network perimeters so that all outgoing web, file transfer protocol (FTP), and secure shell traffic to the Internet shall pass through at least one proxy on a DMZ network.

5.2.35. The proxy shall support logging individual TCP sessions; blocking specific URLs, domain names, and IP addresses to implement a black list (updated daily); and applying white lists of allowed sites that can be accessed through the proxy while blocking all other sites.

5.2.36. Organizations shall force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.

5.2.37. Proxies shall be used to encrypt all traffic leaving an organization.

5.2.38. Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.

5.2.39. All devices remotely logging into the internal network shall be managed by the enterprise, with remote control of their configuration, installed software, and patch levels.

Notes: Does this imply a VPN type of situation, or does it include configuring your iPhone to use the corporate Exchange server? In both cases you have a BYOD problem to consider.

5.2.40. Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.

Notes: If you are looking for unauthorized VPN connections, you are going to need a tight list of access rules to check against. Another interpretation of this requirement might be that you need to check for VPN traffic outbound from your internal network to some non-organizationally provided VPN (like one to Amsterdam). If you are logging all your packets at the boundary (like previous requirements say), then you shall not have a problem looking for common VPN protocols – until you get to an SSL VPN, in which case you are going to need a list of VPN services and their IP addresses to check the traffic.

5.2.41. To limit access by an insider or malware spreading on an internal network, organizations shall devise internal network segmentation schemes to limit traffic to only those services needed for business use across the internal network.

5.2.42. The system shall have the ability to update filtering on internal networks on demand, driven from incident detection and response, to help stop the spread of malware or an intruder.

5.2.43. To minimize the impact of an attacker pivoting between compromised systems, only allow DMZ systems to communicate with private network systems via application proxies or application-aware firewalls over approved channels

5.2.44. To help identify covert channels exfiltrating data through a firewall, built-in firewall session tracking mechanisms included in many commercial firewalls shall be configured to identify TCP sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions.

5.2.45. Deploy NetFlow collection and analysis to DMZ network flows to detect anomalous activity.

Notes: Flows can be invaluable when detecting anomalies. In fact, they shall not be relegated to the DMZ (see http://link.springer.com/chapter/10.1007%2F978-0-387-68768-1_1 for more information).

5.2.46. Packet sniffers shall be deployed on DMZs to look for Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies as well as SMTP, FTP, SSH, and so on.

5.2.47. The system shall be capable of identifying any unauthorized packets sent into or out of a trusted zone and ensure that the packets are properly blocked and/or trigger alerts.

5.2.48. Any unauthorized packets shall be detected within 24 hours, with the system generating an alert or e-mail for enterprise administrative personnel and incident response team.

5.2.49. Alerts shall be sent every hour thereafter until the boundary device is reconfigured.

Mobile Computing Device

To ensure that Mobile Computing Devices (MCDs) do not introduce threats into systems that process or store County information, departments' management will:

5.2.50. Establish and manage a process for authorizing, issuing and tracking the use of MCDs.

5.2.51. Permit only authorized MCDs to connect to County information assets or networks that store, process, transmit, or connects to County information and information assets.

5.2.52. Enforce authentication using two-factor authentication.

5.2.53. Implement applicable access control requirements in accordance with *Section on Access Control*, such as the enforcement of a system or device lockout after 15 minutes of inactivity requiring re-entering of a password to unlock.

5.2.54. Install an encryption algorithm that meets or exceeds industry recommended encryption standard for any MCD that will be used to store County information. See *Section on Encryption*.

5.2.55. Ensure that MCDs are configured to restrict the user from circumventing the authentication process.

5.2.56. Provide security awareness training to County employees that informs MCD users regarding MCD restrictions.

5.2.57. Recommend that users label MCDs with an address or phone number so that the device can be returned to the owner if recovered.

Personally Owned Device

Personal computing devices include, but are not limited to, removable media such as thumb or USB drives, external hard drives, laptop or desktop computers, cellular phones, or personal digital assistants (PDA's) owned by or purchased by SE employees, contract personnel, or other non-state user.

5.2.58. The connection of any computing device not owned by the County to a County network or computing device is prohibited unless previously approved.

5.2.59. The installation of any software, executable, or other file to any County computing device is prohibited if that software, executable, or other file downloaded by, is owned by, or was purchased by an employee or contractor with his or her own funds.

5.2.60. The installation of downloaded software, executables, or other files to any County computing device is prohibited when downloaded or installed by an employee or contractor for personal use. Downloaded software, executable, or other files include, but are not limited to: SKYPE, music files or software, and personal photos.

5.2.61. The County will respect the privacy of a user's voluntary use of a personally owned device to access County IT resources. Users cannot be required and/or can refuse to user their personally owned devices to work on or access County resources.

5.2.62. The County will only request access to the personally owned device and password in order to implement security controls; to respond to litigation hold (aka: e-discovery) requests arising out of administrative, civil, or criminal directives, Public Record Act requests, and subpoenas; or as otherwise required or permitted by applicable state or federal laws. Such access will be performed by an authorized technician or designee using a legitimate software process.

Logon Banners and Warning Notices

5.2.63. All computer systems at initial connection to County network shall display warning banners informing potential users of conditions of use consistent with state and federal laws.

5.2.64. Warning banners shall remain on the screen until the user takes explicit actions to log on to the information system.

5.2.65. The banner message will be placed at the user authentication point for every computer system that connects to the County network. The banner message may be placed on an initial logon screen in situations where the logon provides access to multiple computer systems.

5.2.66. At a minimum, banner messages shall provide appropriate privacy and security information and shall contain information informing potential users that:

5.2.67. User is accessing a government information system for conditions of use consistent with state and federal information security and privacy protection laws.

5.2.68. System usage may be monitored, recorded, and subject to audit.

5.2.69. Unauthorized use of the system is prohibited and subject to criminal and civil penalties.

5.2.70. Use of the system indicates consent to monitoring and recording.

Authentication

5.2.71. Authenticate user identities at logon. Authentication mechanisms will be appropriate to the sensitivity of the information.

Single Sign-On Systems

Single Sign-On, or SSO systems are mechanisms that allow a user to authenticate to one authentication authority and gain access to multiple applications or systems that have different authentication mechanisms. User credentials for their multiple applications are usually stored and securely managed by the SSO system. Although SSO systems could provide a vector for unauthorized access if compromised, properly implemented and maintained SSO systems can provide additional security in the form of two-factor authentication and fewer forgotten passwords.

5.2.72. All SSO systems shall meet Federal Information Security Management Act (FISMA) and Federal Risk and Authorization Management Program (FedRAMP) standards.

5.2.73. The controlling authentication mechanism for any SSO system shall be preceded with some form of two-factor authentication that is also FISMA and FedRAMP compliant.

5.2.74. If credentials are stored, they shall be encrypted with FIPS 140-2 validated cryptographic modules.

5.2.75. Stored credentials cannot be accessible by administrators of the system.

Multi-Factor Authentications

5.2.76. Multi-Factor Authentication, or MFA, is a method of using multiple separate pieces of information for authentication. These are generally said to be something you have, and something you know. In single-factor authentication, a user ID and password are things you know. With MFA, a token or biometric feature is used as an additional factor as something you have. MFA shall be required for external connections unless otherwise approved.

Notes: Employing the use of two separate user ID's and passwords does not meet this standard.

5.2.77. Multi-Factor Authentication may be required for access to sensitive (as defined by County Policy) data.

Password Standards

Passwords are the first line of protection for user accounts. Poorly managed passwords could become the weakest security link and may result in the compromise of County information and information assets. These standards establish the minimum requirements to create and to maintain a secure environment.

Password Requirements Enforced by Systems

5.2.78. Passwords shall contain at least eight characters. For systems that cannot accept a password of eight characters, a variance request shall be completed and submitted per the *County Variance Review and Approval Process*.

5.2.79. Passwords shall be required to have a minimal age of one day,

5.2.80. The system shall automatically require the password to be changed every 90 days.

5.2.81. Passwords shall satisfy the complexity rule:

- Passwords will contain a minimum of two upper case letters
- Passwords will contain a minimum of two lower case letters
- Passwords will contain a minimum of two numbers: 1- 0
- Passwords will contain a minimum of two symbols: !,@,#,$,%,^,&,*,(,)
- Password characters will not be sequential (Do not use: ABCD , This is ok: ACDB)

- Passwords characters will not be repeated in a row (Do not use: P@$$S. This is ok: P@S)
- COMPLEX PASSWORD EXAMPLE: P@$SWoRd13

5.2.82. Passwords shall not be reused for twelve iterations.

5.2.83. Secure password delivery and password reset mechanisms to assure passwords are known only to the user.

5.2.84. The user account shall be automatically disabled after five unsuccessful logon attempts. Users with locked accounts shall contact their local systems administrator or the central IT service desk as applicable per the department's local IT management policies to have their account unlocked and password reset.

5.2.85. After a user password reset, the system shall require the user to change password at the first logon attempt following the reset.

5.2.86. Passwords files shall be encrypted using one way hashing algorithms to prevent compromise and disclosure when stored in files or databases on systems and servers. Microsoft's Local Area Network Manager (LM) and NT Local Area Network Manager (NTLM) hash shall not be used to store passwords as these files are easily compromised. If passwords cannot be encrypted, access to the file or database element containing the passwords shall be restricted to authorized system administrators.

5.2.87. Before deploying any new devices in a networked environment, departments shall change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to comply with password requirements. Refer to *Section on Passwords*.

Inactivity Timeout and Restricted Connection Times

5.2.88. Automatic lockouts for system devices, including workstations or other mobile computing devices, after no more than 15 minutes of inactivity. Refer to *Section on Mobile Computing Device*.

5.2.89. Automatic network session termination for network connections associated with a communications session at the end of a session after no more than 15 minutes of inactivity.

Account Monitoring

5.2.90. Review all system accounts and disable any account that cannot be associated with a business process and owner.

5.2.91. All accounts shall have an expiration date associated with the account.

5.2.92. Systems shall automatically create a report on a daily basis that includes a list of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire.

5.2.93. The list shall be sent to the associated system administrator in a secure fashion.

5.2.94. Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor.

5.2.95. Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

5.2.96. Monitor account usage to determine dormant accounts that have not been used for a given period, such as 45 days, notifying the user or user's manager of the dormancy.

5.2.97. After a longer period, such as 60 days, the account shall be disabled.

5.2.98. When a dormant account is disabled, any files associated with that account shall be encrypted and moved to a secure file server for analysis by security or management personnel.

5.2.99. On a periodic basis, such as quarterly or at least annually, organizations shall require that managers match active employees and contractors with each account belonging to their managed staff.

5.2.100. Security or system administrators shall then disable accounts that are not assigned to active employees or contractors.

5.2.101. Monitor attempts to access deactivated accounts through audit logging.

5.2.102. Profile each user's typical account usage by determining normal time-of-day access and access duration for each user.

5.2.103. Daily reports shall be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration by 150 percent.

5.2.104. This includes flagging the use of user's credentials from a computer other than computers usually used by the user.

5.2.105. The system shall be capable of identifying unauthorized user accounts when they exist on the system.

5.2.106. An automated list of user accounts on the system shall be created every 24 hours and an alert or e-mail shall be sent to administrative personnel within one hour of completion of a list being created.

5.2.107. The evaluation team shall verify that the list of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire has successfully been completed on a daily basis for the previous 30 days by reviewing archived alerts and reports to ensure that the lists were completed.

5.2.108. A comparison of a baseline of allowed accounts shall be compared to the accounts that are active in all systems. The report of all differences shall be created based on this comparison.

Monitoring System Access and Use

5.2.109. Provide accountability for each user's activity involving sensitive (as defined by County Policy) information by enforcing detailed audit logging of access to sensitive data.

5.2.110. Audit logging will be enabled to detect invalid login attempts.

5.2.111. The system shall be capable of detecting and logging attempts by users to access files on local systems or network-accessible file shares without the appropriate privileges

5.2.112. The system shall generate an alert or e-mail to administrative personnel within 24 hours.

Administrative Privileges

5.2.113. Use automated tools to inventory all administrative/service accounts.

5.2.114. Use automated tools to validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.

5.2.115. Privileged user accounts are only granted to authorized individuals with a business need for the privileged access.

5.2.116. Users with privileged user accounts shall have two user IDs: one for normal day-to-day activities and one for performing administrator duties.

5.3.1. Administrators may only use their administrator account to perform administrator functions. For example, do not login with administrative account when using the system as a regular user, not performing administrative duties.

5.2.117. Privileged user accounts shall not have internet access.

5.2.118. Administrators may not use their privileged access for unauthorized viewing, modification, copying, or destruction of system or user data.

5.2.119. Configure all administrative-level accounts' passwords to comply with *Section on Passwords*.

5.2.120. Configure all administrative-level accounts to require regular password changes in compliance with password requirements. Refer to *Section on Passwords*.

5.2.121. Passwords for all systems shall be stored in a well-hashed or encrypted format, with weaker formats eliminated from the environment.

Notes: Rule of thumb is *never use anything that is reversible to store passwords*. Salted hash.

5.2.122. Furthermore, files containing these encrypted or hashed passwords required for systems to authenticate users shall be readable only with super-user privileges.

5.2.123. Departments shall also monitor these files for change and verbosely log all access to the file.

5.2.124. Utilize access control lists to ensure that administrator accounts are used only for system administration activities, and not for reading e-mail, composing documents, or surfing the Internet.

5.2.125. Web browsers and e-mail clients especially shall be configured to never run as administrator.

5.2.126. Through policy and user awareness, require that administrators establish unique, different passwords for their administrator and non-administrator accounts.

5.2.127. Administrative accounts shall never be shared.

5.2.128. Users shall only use the Windows “administrator” or Unix “root” accounts in emergency situations.

5.2.129. Domain administration accounts shall be used when required for system administration instead of local administrator accounts.

5.2.130. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior (e.g., system reconfigurations during the night shift).

5.2.131. Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators group.

5.2.132. All administrative access, including domain administrative access, shall use two-factor authentication.

5.2.133. Access to a machine (either remotely or locally) shall be blocked for administrator-level accounts. Instead, administrators shall be required to access a system using a fully logged and non-administrative account. Then, once logged in to the machine without administrative privileges, the administrator shall transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.

5.2.134. If services are outsourced to third parties, language shall be included in the contracts to ensure that they properly protect and control administrative access.

5.2.135. It shall be validated that they are not sharing passwords and have accountability to hold administrators liable for their actions.

5.2.136. Additionally, security personnel shall be notified via an alert or e-mail within 24 hours of the addition of an account to a super-user group, such as a domain administrator.

Remote Access

Remote Access Authorization

5.2.137. Departments shall develop a Remote Access authorization process to ensure Remote Access to County information and information assets is granted based on business needs. This process shall include a “Remote Access Request Form” that requires the user to detail the access needed, describe the business need, and certify knowledge and acceptance of this standard. The form shall also detail acceptable use policies and consequences of unauthorized access or disclosure.

5.2.138. The Remote Access solution shall leverage end to end encryption such as Virtual Private Network (VPN) or Secure Socket Link (SSL).

5.2.139. The Remote Access solution shall ensure that the user credentials are exchanged in an encrypted format.

5.2.140. Departments shall monitor remote access to ensure compliance with requirements and appropriate use.

5.2.141. Remote access shall only be allowed from devices owned, managed, and controlled by the applicable organization with the following exception:

- Personally owned or non-applicable organization owned devices may be used only to access web based applications (such as e-mail and calendar services) containing information classified as sensitive (as defined by County Policy).

Notes: Information classified as sensitive (as defined by County Policy) may NOT be accessed using personally owned or non-applicable organization owned devices (i.e. Devices owned by court facilities, public libraries, airports, or privately owned businesses).

Remote Access System Requirements

5.2.142. All remote access shall be authenticated using Multi Factor Authentication.

5.2.143. If applicable, remote access users and equipment shall comply with Mobile Computing Device requirements. Refer to *Section on Mobile Computing Device*.

5.2.144. Remote access equipment shall comply with Encryption Standard. Refer to *Section on Encryption.*

5.2.145. Remote access using wireless connections shall comply with Wireless Access Control requirements. Refer to *Section on Wireless Access Control*.

Remote Access Configuration Requirements

5.2.146. Equipment used for remote access to County information and County information assets shall be configured securely according to the following:

5.2.147. Screen saver shall automatically activate after ten minutes and require a password.

5.2.148. Antivirus software shall be installed, enabled for “real-time” scans, enabled for automatic anti-virus definition updates.

5.2.149. “Critical” or “Security” software patches shall be installed to ensure that software is kept current.

5.2.150. Systems shall only contain software authorized by department/County.

5.2.151. All unnecessary services and ports shall be disabled.

5.2.152. Only enable TCP/IP protocol.

5.2.153. Unnecessary ports on the personal firewall shall be disabled or blocked.

5.2.154. File sharing and/or peer-to-peer programs are strictly prohibited.

5.2.155. Apply security best practices as recommended by the National Institute of Standards and Technology (NIST).

Remote Access Requirements

5.2.156. Obtain management approval prior to using remote access services.

5.2.157. Have a legitimate business need for remote access to County information or information assets.

5.2.158. Use remote access services only for County business.

5.2.159. Agree to the requirements detailed in this standard by signing the Remote Access Request Form.

Remote Access Documentation

5.2.160. All departments that authorize remote access to County information and information assets will implement a process to manage remote access. The process will include:

5.2.161. Procedures to verify that only users with a legitimate business need are authorized for remote access.

5.2.162. Procedures to verify that remote access is removed or disabled when the user no longer requires remote access.

5.2.163. Procedures to ensure that Remote Access Request Forms are retained and made available to OCIT Enterprise Security upon request.

5.2.164. A tracking system to monitor remote access.

5.2.165. Audit procedures to ensure adherence to the above standards.

Wireless Access Control

5.2.166. Ensure that each wireless device connected to the network matches an authorized configuration and security profile.

5.2.167. Ensure the authorized configuration and security profile contains documented owner of the connection and a defined business need.

5.2.168. Organizations shall deny access to those wireless devices that do not have such a configuration and profile.

5.2.169. Ensure that all wireless access points are manageable using enterprise management tools. Access points designed for home use often lack such enterprise management capabilities, and shall therefore be avoided in enterprise environments.

5.2.170. Network vulnerability scanning tools shall be configured to detect wireless access points connected to the wired network.

5.2.171. Identified devices shall be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points shall be deactivated.

5.2.172. Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises.

5.2.173. In addition to WIDS, all wireless traffic shall be monitored by IDS as traffic passes into the wired network.

5.2.174. 802.1x shall be used to control which devices are allowed to connect to the wireless network.

5.2.175. A site survey shall be performed to determine what areas within the organization need coverage.

5.2.176. After the wireless access points are strategically placed, the signal strength shall be tuned to minimize leakage to areas that do not need coverage.

5.2.177. Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks.

5.2.178. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface), with password protections to lower the possibility that the user will override such configurations.

5.2.179. Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least WiFi Protected Access 2 (WPA2) protection.

5.2.180. Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.

5.2.181. Ensure that wireless clients use strong, multi-factor authentication credentials to mitigate the risk of unauthorized access from compromised credentials.

5.2.182. Disable peer-to-peer wireless network capabilities on wireless clients, unless such functionality meets a documented business need.

5.2.183. All mobile devices, including personnel devices, shall be registered prior to connecting to the wireless network.

Notes: Already covered by requiring that some method of authentication is in place for networks and devices (remember the 802.1x stuff?). Of course, the added wrinkle here is that it includes BYOD. That means that you are going to need to rely on your end users to do the right thing.

5.2.184. All registered devices shall be scanned and follow the corporate policy for host hardening and configuration management.

Notes: This is great for corporate devices, but probably will not fly for BYOD devices. I would have an entirely separate wireless network for BYOD and allow VPN from there.

5.2.185. Configure all wireless clients used to access private networks or handle organization data in a manner so that they cannot be used to connect to public wireless networks or any other networks beyond those specifically allowed by the organization.

5.2.186. Departments shall employ wireless scanning, detection, and discovery tools as well as wireless intrusion detection systems.

5.2.187. The security team shall periodically capture wireless traffic from within the borders of a facility and use free and commercial analysis tools to determine whether the wireless traffic was transmitted using weaker protocols or encryption than the organization mandates.

5.2.188. When devices relying on weak wireless security settings are identified, they shall be reported as security incidents. They shall be found within the organization's asset inventory and either reconfigured more securely or denied access to the organization network.

5.2.189. The security team shall employ remote management tools on the wired network to pull information about the wireless capabilities and devices connected to managed systems.

5.2.190. The system shall be capable of identifying unauthorized wireless devices or configurations when they are within range of the organization's systems or connected to their networks.

5.2.191. The system shall be capable of identifying any new unauthorized wireless devices that associate or join the network within one hour.

5.2.192. The system shall alert or e-mail a list of enterprise personnel after unauthorized wireless device detection.

5.2.193. The system shall automatically isolate an attached wireless access point from the network within one hour.

5.2.194. The system shall alert or e-mail a list of enterprise personnel after unauthorized wireless device isolation is achieved.

5.2.195. Every 24 hours after that point, the system shall alert or send e-mail about the status of the system until it has been removed from the network.

5.2.196. The asset inventory database and alerting system shall be able to identify the location, department, and other details of where authorized and unauthorized wireless devices are plugged into the network.

Network Monitoring

5.2.197. Departments shall utilize the County Security Operations Center to monitor its network for potential security incidents.

5.2.198. Deploy network access control (NAC) to monitor authorized systems so if attacks occur, the impact can be remediated by moving the untrusted system to a virtual local area network that has minimal access.

Notes: Alternatively, consider the Security Configuration Management (SCM) profile of a given asset. If an attack is underway (again, something the NAC will not really be responsible for detecting), then the SCM profile may change and be assessed dynamically. When that happens, if the profile for the target asset is unacceptable, then the NAC shall be engaged.

Maintenance, Monitoring, and Analysis of Audit Logs

5.2.199. Each organization shall include at least two synchronized time sources (i.e., Network Time Protocol or NTP) from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Notes: If you use one internal and another external, be sure the one you use internally does not reference the same external NTP source the others are using. A 'regular' basis is something that you will need to determine for your organization. What you need to be concerned with is your 'drift' tolerance. Default tolerance for Kerberos in Windows is five minutes. Consult benchmark sources for specific guidance.

5.2.200. Validate audit log settings include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction (i.e., any user-specific and/or application-specific information).

5.2.201. Systems shall record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools shall be deployed to convert logs into such a format.

5.2.202. On a periodic basis, review all systems that store logs to ensure they have adequate storage space for the logs generated to prevent the log files from filling up between log rotation intervals.

5.2.203. The logs shall be archived on a periodic basis. The logs shall be archived with a well-defined process and audit trail.

Notes: Ideally, the logs shall be digitally signed; however, it may not be feasible for departments to digitally sign. There are other ways to ensure the integrity of the logs. Departments shall evaluate the methods that are right for them.

5.2.204. Log retention shall comply with County Records Management Policy to ensure that the logs are kept for a sufficient period of time (refer to County records retention schedule).

Notes: As APT (advanced persistent threat) continues to stealthily break into systems, organizations are often compromised for several months without detection. The logs need to be kept for a longer period of time than it takes an organization to detect an attack so it can accurately determine what occurred. If you believe your organization is prone to advanced attacks, then you might want to retain logs from a wider set of your assets for a longer period of time (it depends on how slow and low you believe your adversaries to be, and a balance between that and e-discovery requirements).

5.2.205. Monitor special privilege access, e.g. Administration accounts.

5.2.206. Log all modifications to the system files.

5.2.207. Maintain audit logs on a device separate from the system being monitored.

5.2.208. All remote access (i.e., VPN, dial-up, or other mechanism) to a network, whether to the DMZ or the internal network, shall be logged verbosely.

5.2.209. Operating systems shall be configured to log access control events associated with a user attempting to access a resource (e.g., a file or directory) without the appropriate permissions.

5.2.210. Failed logon attempts shall also be logged.

5.2.211. Security personnel and/or system administrators shall run biweekly reports that identify anomalies in logs. They shall then actively review the anomalies, documenting their findings.

5.2.212. Network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, shall be configured to verbosely log all traffic (both allowed and blocked) arriving at the device.

5.2.213. For all servers, organizations shall ensure that logs are written to write-only devices or to dedicated logging servers running on separate machines from hosts generating the event logs, lowering the chance that an attacker can manipulate logs stored locally on compromised machines.

5.2.214. Deploy a SIM/SEM (security incident management/security event management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis.

5.2.215. Using the SIM/SEM tool, system administrators and security personnel shall devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.

5.2.216. Carefully monitor for service creation events. On Windows systems, many attackers use psexec functionality to spread from system to system. Creation of a service is an unusual event and needs to be monitored closely.

5.2.217. The system shall be capable of logging all events across the network.

5.2.218. The logging shall be validated across both network-based and host-based systems.

5.2.219. Any event shall generate a log entry that includes a date, timestamp, source address, destination address, and other details about the packet.

5.2.220. When a device detects that it is not capable of generating logs (due to a log server crash or other issue), it shall generate an alert or e-mail for enterprise administrative personnel.

Malware Defenses

5.2.221. Endpoint security software shall implement white and black lists of programs allowed to run or blocked from executing.

5.2.222. Departments shall implement anti-virus, anti-spyware, personal firewall, and host- based intrusion detection systems (IDS) and intrusion prevention systems (IPS), along with application white and black listing.

5.2.223. Endpoint security software shall look at the name, file system location, and/or cryptographic hash of a given executable to determine whether the application shall be allowed to run on the protected machine.

5.2.224. Security tools shall utilize custom white and black lists based on executable path, hash, or regular expression matching. Department administrators shall define rules for execution of specific programs only by certain users and at certain times of day, and black lists based on specific signatures.

5.2.225. The system shall be capable of identifying unauthorized software by detecting an attempt to install it.

Notes: Most installed software needs some elevated privilege to run, and many modern systems provide some level of protection around installing such software.

5.2.226. System shall be capable of identifying unauthorized software by detecting an attempt to execute it.

Notes: This means that some process is looking at the application trying to start, assessing it against a list of known good software, and then taking some action.

5.2.227. The system shall be capable of notifying enterprise administrative personnel within 24 hours through an alert or e-mail.

5.2.228. Systems shall block installation, prevent execution, or quarantine unauthorized software.

5.2.229. Systems shall alert or send e-mail when blocking, preventing, or quarantining action has occurred.

5.2.230. Every 24 hours after that point, the system shall alert or send e-mail about the status of the system until the unauthorized system has been removed from the network.

5.2.231. Employ automated tools to continuously monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection including anti-virus, anti- spyware, personal firewalls, and host-based IPS functionality.

5.2.232. All malware detection events shall be sent to enterprise anti-malware administration tools.

5.2.233. All malware detection events shall be sent to enterprise event log servers.

5.2.234. The endpoint security solution shall include zero-day protection such as network behavioral heuristics.

5.2.235. Employ anti-malware software and signature auto-update features or have administrators manually push updates to all machines on a daily basis.

5.2.236. After applying an update, automated systems shall verify that each system has received its signature update.

5.2.237. Configure laptops, workstations, and servers so that they will not auto-run content from USB tokens (i.e. “thumb drives”), USB hard drives, CDs/DVDs, Wi-Fi devices, external serial advanced technology attachment devices, mounted network shares, or other removable media.

5.2.238. If the devices are not required for business use, they shall be disabled.

5.2.239. Configure systems so that they conduct an automated anti-malware scan of removable media when it is inserted.

5.2.240. All e-mail content entering the organization’s e-mail gateway shall be scanned prior to being placed in the recipients’ inbox.

5.2.241. E-mail containing malicious content shall be quarantined and the recipient prevented from opening it.

5.2.242. All e-mail attachments entering the organization’s e-mail gateway shall be scanned prior to being placed in the recipients’ inbox.

5.2.243. E-mail attachments determined to contain malicious code or having file types unneeded for the organization’s business shall be quarantined.

5.2.244. All Web content entering the organization’s Web Proxy (or perimeter if no such proxy exists) shall be scanned for malicious content before being delivered to the user agent.

5.2.245. Web content containing malicious content shall be blocked from delivery to the user agent.

5.2.246. Departments shall apply anti-virus scanning at the Web Proxy gateway.

5.2.247. Content filtering for file-types shall be applied at the perimeter.

5.2.248. Deploy features and toolkits that prevent malware exploitation. For example, Data Execution Prevention (DEP) and Enhanced Mitigation Experience Toolkit (EMET), products that provide sandboxing (e.g., run browsers in a VM), and other techniques that prevent malware exploitation.

5.2.249. Limit use of external devices to those that have business need. Monitor for use and attempted use of external devices.

5.2.250. Block access to external e-mail systems

5.2.251. Block access to external instant messaging services.

5.2.252. Block access to other external social media tools

5.2.253. Automated monitoring tools shall use behavior-based anomaly detection to complement and enhance traditional signature-based detection.

5.2.254. Utilize network-based anti-malware tools to analyze all inbound traffic and filter out malicious content before it arrives at the endpoint.

5.2.255. Departments shall monitor all inbound and outbound traffic.

5.2.256. Any unauthorized traffic shall be reported as a security incident and investigated.

5.2.257. Unauthorized traffic determined as malicious shall result in the computer being moved to an isolated VLAN.

Notes: This is an excellent opportunity for NAC integration. If your detection capability can direct your NAC capability, this migration to an isolated VLAN can be automatic.

5.2.258. Any large transfers of data shall be held until validated.

5.2.259. Large transfers of data determined as malicious shall result in the computer being moved to an isolated VLAN.

Notes: This is an excellent opportunity for NAC integration. If your detection capability can direct your NAC capability, this migration to an isolated VLAN can be automatic.

5.2.260. Implement an incident response process that allows their IT Support Organization to supply their Security Team with samples of malware running undetected on corporate systems.

Notes: require IT operations to image the machine in question and hand that image over to the Security Team with as much supporting information as possible.

5.2.261. Departments shall work with security vendors to create signatures. For example, providing samples to the security vendor for “out-of- band” signature creation and subsequent deployment to the enterprise by system administrators.

5.2.262. Utilize network-based flow analysis tools to analyze inbound and outbound traffic looking for anomalies, indicators of malware, and compromised systems.

5.2.263. Deploy “reputation-based technologies” on all endpoint devices to cover the gap of signature-based technologies.

5.2.264. Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.

5.2.265. Apply proxy technology to all communication between internal network and the Internet.

5.2.266. Some enterprises deploy free or commercial honeypot and tarpit tools to identify attackers in their environment.

5.2.267. The system shall identify any malicious software installed on a computer system within one hour.

5.2.268. The system shall identify any malicious software attempted to be installed on a computer system within one hour.

5.2.269. The system shall identify any malicious software executed on a computer system within one hour.

5.2.270. The system shall identify any malicious software attempted to be executed on a computer system within one hour.

5.2.271. The system shall alert or e-mail notification to a list of enterprise personnel via their centralized anti-malware console or event log system.

5.2.272. Systems shall block installation, prevent execution, or quarantine malicious software within one hour.

5.2.273. Systems shall alert or e-mail when such blocking, prevention, or quarantine has taken place.

5.2.274. Every 24 hours after that point, the system shall alert or send e-mail about the status of the malicious code until such time as the threat has been completely mitigated on that system.

Data Loss Prevention

5.2.275. Host-based data loss prevention (DLP) shall be used to enforce ACLs even when data is copied off a server.

5.2.276. Deploy approved hard drive encryption software to mobile devices.

5.2.277. Deploy approved hard drive encryption software to devices processing, storing, or transmitting sensitive (as defined by County Policy) information.

5.2.278. Deploy an automated tool on network perimeters that monitors for certain sensitive (as defined by County Policy) information (i.e., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.

5.2.279. Conduct periodic scans of server machines using automated tools to determine whether sensitive data (i.e., personally identifiable information, health, credit card, and classified information) is present on the system in clear text.

5.2.280. Sensitive (as defined by County Policy) data shall be moved between networks using secure, authenticated, and encrypted mechanisms.

5.2.281. If there is no business need for supporting such devices, organizations shall configure systems so that they will not write data to USB tokens or USB hard drives.

5.2.282. If such devices are required, enterprise software shall be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices.

5.2.283. An inventory of all authorized devices shall be maintained.

5.2.284. Use network-based DLP solutions to monitor and control the flow of data within the network.

5.2.285. Any anomalies that exceed the normal traffic patterns shall be noted and appropriate action taken to address them.

5.2.286. Monitor all traffic leaving the organization and detect any unauthorized use of encryption.

5.2.287. Block access to known file transfer and e-mail exfiltration websites.

Notes: Subscribe to a service that offers these lists. Ensure the tools you use understand how to import those lists.

5.2.288. The system shall be capable of identifying unauthorized data leaving the organization, whether via network file transfers or removable media.

5.2.289. Enterprise administrative personnel shall be alerted by the appropriate monitoring system of a data exfiltration event or attempt.

5.2.290. Once the alert has been generated it shall also note the system and location where the event or attempt occurred.

5.2.291. If the system is in the organization's asset management database, the system owner shall also be included in the generated alerts.

5.2.292. Every 24 hours after that point, the system shall alert or send e-mail about the status of the systems until the source of the event has been identified and the risk mitigated.

Secure Data Transfer

5.2.293. All data transfers to an external entity require an approved agreement be in place prior to commencing data transfer. Approved agreements can be contracts, inter-agency agreements (IAAs), memorandum of understanding (MOUs), service level agreements (SLAs), or other binding forms or documents.)

Data Transfer Information Owner Requirements

5.2.294. Review requested data transfers and ensure they are necessary for legitimate business purposes.

5.2.295. Identify the external entity to which County information is to be transferred.

5.2.296. Identify the data source (e.g., physical location, system or application, etc.).

5.2.297. Identify the method of transferring the data.

5.2.298. Identify how long external entity shall retain the data sent to them.

5.2.299. Identify security and privacy risks of data prior to approving data transfer.

5.2.300. Consider security measures of external entities as a key component of evaluation and selection for acquiring an external entity to provide services or support for data transfers.

5.2.301. Ensure data sharing or exchange agreements include defined requirements for processes and procedures for security protection measures for meeting acceptable levels of data security and privacy protection prior to transferring data.

5.2.302. Ensure external entity has a contractual agreement or other binding form or documents with applicable organization in accordance with the section entitled Data Transfer Agreement Requirements below.

5.2.303. Require external parties to return all County information or certify in writing of the destruction of all County information when they are no longer needed for the business purpose for which they were obtained or agreed upon period of time of data retention in compliance with County Records Management Policy or termination of agreement (refer to County records retention schedule).

Data Transfer Information Custodian Requirements

5.2.304. The County information custodian shall maintain the security and confidentiality of County information and ensure the implementation of security controls prescribed by the information owner. County information custodians shall ensure:

5.2.305. Data transfers have prior written approval by applicable organization’s information owner.

5.2.306. Data transfers have prior approval from applicable organization’s information security officer.

5.2.307. All electronic County Information transferred to an external entity uses methods of encryption in accordance with Encryption Standards. Refer to *Section on Encryption*.

5.2.308. This includes data transfers via the use of e-mail, FTP or any portable storage media (e.g., CD, DVD, USB flash drive, etc.).

5.2.309. A method is in place to terminate data transfers.

5.2.310. The use of fax machines to transmit data is avoided whenever possible.

5.2.311. Multiple layers of security mechanisms shall be in place to ensure accurate sending and receipt of transferred data. (Examples include but not limited to the use of a fax cover sheet with a statement of the confidentiality of the data, the need for protection, and notice to unintended recipients to telephone the sender; ensuring trusted personnel are located at both the sending and receiving fax machines; and validating receipt of the fax by contacting external entity, etc.).

5.2.312. Ensure receipt of data transferred.

5.2.313. Records or logs that document the data transfer shall be retained and made available to the County for up to six (6) years. Documentation or records shall include information that verifies what data was transferred, the destination of the data, and acknowledgement of receipt of data.

5.2.314. Automated data transfers that run without manual interventions whatsoever other than to start the automated transfer process have a termination date.

5.2.315. An action plan for notification for any information security breach involving County information is in place in accordance with *Section 3.2.5 – Incident Management*.

Encryption

Departments shall develop procedures to implement the following requirements to protect County information classified as sensitive (as defined by County Policy):

5.2.316. Encrypt when stored on portable computing devices i.e. Laptops, PDAs, etc.

5.2.317. Encrypt when stored on portable storage media i.e. CDs, DVDs, USB flash drives, tapes, removable hard drives, etc.

5.2.318. Encrypt when transmitted over a public network. Solutions may include: Secure Socket Layer (SSL), Virtual Private Network (VPN), Secure File Transfer Protocol (SFTP), encrypted e-mail, and/or encrypted wireless networks.

5.2.319. Ensure contractors such as business partners or vendors provide the same controls and safeguards to protect sensitive (as defined by County Policy) County information.

5.2.320. When an encryption product is employed, it shall be certified according to Federal Information Processing Standards (*FIPS Publication 140-2*). Use of proprietary encryption algorithms is not allowed for any purpose on County information or County information assets.

5.2.321. Encrypt using at a minimum a 128-bit randomly generated key. The encryption algorithm shall meet or exceed the current industry standard of Triple DES. However, departments are encouraged to leverage the latest standard approved by the National Institute of Standards and Technology (NIST), such as AES for future implementations.

5.2.322. All communication of sensitive (as defined by County Policy) information shall be encrypted.

Penetration Tests and Red Team Exercises

5.2.323. Conduct regular external and internal penetration tests (every three to five years) to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.

5.2.324. Penetration testing shall occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.

Notes: Involve County Counsel to review contracts and scope of work.

5.2.325. If any user or system accounts are used to perform penetration testing, those accounts shall be carefully controlled and monitored to make sure they are only being used for legitimate purposes.

Notes: Enforce separation of duties during the penetration testing. Document what you are going to do, what you are doing, and what you have done.

5.2.326. Perform periodic red team exercises to test the readiness of organizations to identify and stop attacks or to respond quickly and effectively.

5.2.327. Ensure that systemic problems discovered in penetration tests and red team exercises are fully tracked and mitigated.

5.2.328. Set up automated processes to find: Clear text e-mails and documents with "password" in the filename or body.

5.2.329. Set up automated processes to find: Critical network diagrams stored online and in clear text.

5.2.330. Set up automated processes to find: Critical configuration files stored online and in clear text.

5.2.331. Set up automated processes to find: Vulnerability assessment, penetration test reports, and red team finding documents stored online and in clear text.

5.2.332. Set up automated processes to find: Other sensitive (as defined by County Policy) information identified by management personnel as critical to the operation of the enterprise during the scoping of a penetration test or red team exercise.

5.2.333. Social engineering shall be included within a penetration test. The human element is often the weakest link in an organization and one that attackers often target.

5.2.334. Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectors, often social engineering combined with web or network exploitation. Red team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets.

5.2.335. Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments shall be used as a starting point to guide and focus penetration testing efforts.

5.2.336. Devise a scoring method for determining the results of red team exercises so that results can be compared over time.

5.2.337. Create a test bed that mimics a production environment for specific penetration tests and red team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.

Secure SDLC

5.2.338. Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks.

5.2.339. Web application protection shall include cross-site scripting attacks, SQL injection attacks, command injection attacks, and directory traversal attacks.

5.2.340. For applications that are not web-based, specific application firewalls shall be deployed if such tools are available for the given application type.

5.2.341. If the traffic is encrypted, the device shall either sit behind the encryption or be capable of decrypting the traffic prior to analysis.

Notes: The most secure architectures will be unable to decrypt everything, but that shall still be OK. The goal here is to find the middle ground appropriate for the application and mission that balances security with usability/function.

5.2.342. If neither option is appropriate, a host-based web application firewall shall be deployed.

Notes: In other words, the Web/non-Web application firewall shall not reside on the host, but may if there is no other solution.

5.2.343. At a minimum, explicit error checking shall be done for all input.

5.2.344. Whenever a variable is created in source code, the size and type shall be determined.

5.2.345. When input is provided by the user, it shall be verified that it does not exceed the size or the data type of the memory location in which it is stored or moved in the future.

5.2.346. Test Web applications for common security weaknesses using automated remote web application scanners prior to deployment.

5.2.347. Test Web applications (in-house-developed and third-party-procured) for common security weaknesses using automated remote web application scanners on a regular recurring basis and whenever updates are made to the application.

5.2.348. Organizations shall understand how their applications behave under denial of service attacks, and test the application for load/resource constraints and have an executable plan in place for when something goes wrong.

5.2.349. System error messages shall not be displayed to end-users (output sanitization).

5.2.350. Maintain separate environments for production and nonproduction systems.

5.2.351. Developers shall not have unmonitored access to production environments.

5.2.352. Test web and other application software (in-house-developed and third-party-procured) for coding errors and malware insertion prior to deployment using automated static code analysis software. Such testing shall include back doors.

5.2.353. If source code is not available, test compiled code using static binary analysis tools.

5.2.354. In particular, input validation and output encoding routines of application software shall be carefully reviewed and tested.

5.2.355. For applications that rely on a database, organizations shall conduct a configuration review of both the operating system housing the database and the database software itself, checking settings to ensure that the database system has been hardened using standard hardening templates.

5.2.356. Ensure that all software development personnel receive training in writing secure code for their specific development environment.

5.2.357. Sample scripts, libraries, components, compilers, or any other unnecessary code that is not being used by an application shall be uninstalled or removed from the system.

5.2.358. Organizations shall use CWE to determine which types of weaknesses they are most interested in addressing and removing.

5.2.359. When evaluating the effectiveness of testing for these weaknesses, MITRE's Common Attack Pattern Enumeration and Classification shall be used to organize and record the breadth of the testing for the CWEs and to enable testers to think like attackers in their development of test cases.

5.2.360. The WAF shall be capable of detecting and blocking an application-level software attack.

5.2.361. The WAF shall generate an alert or send e-mail to enterprise administrative personnel within 24 hours of detection and blocking.

5.2.362. All Internet-accessible web applications shall be scanned, at a minimum, on a monthly basis.

5.2.363. All Internet-accessible web application scans shall alert or send an e-mail to administrative personnel within 24 hours of completing a scan.

5.2.364. If a scan cannot be completed successfully, the system shall alert or send e-mail to administrative personnel within one hour indicating that the scan has been unsuccessful.

5.2.365. Every 24 hours after that point, the system shall alert or send e-mail about the status of uncompleted scans, until normal scanning resumes.

5.2.366. Additionally, all high-risk vulnerabilities in Internet-accessible web applications identified by web application vulnerability scanners shall be mitigated (by either fixing the flaw or implementing a compensating control) within 30 days of discovery of the flaw.

5.2.367. Additionally, all high-risk vulnerabilities in Internet-accessible web applications identified by static analysis tools, shall be mitigated (by either fixing the flaw or implementing a compensating control) within 30 days of discovery of the flaw.

5.2.368. Additionally, all high-risk vulnerabilities in Internet-accessible web applications identified by automated database configuration review tools shall be mitigated (by either fixing the flaw or implementing a compensating control) within 30 days of discovery of the flaw.

5.2.369. The web application vulnerability scanner shall be configured to assess all of the organization's Internet-accessible web applications to identify such errors.

Application Access Control

For any system that processes or stores sensitive (as defined by County Policy) information, controls shall be used to restrict access within application systems. Logical access to software and information shall be limited to authorized users only. Application system controls shall:

5.2.370. Control user access to information and application system functions, according to a defined access-control policy.

5.2.371. Prevent unauthorized access to any utility or operating-system software that can override system or application controls.

5.2.372. Prevent compromise to the security of other systems with which information resources are shared.

5.2.373. Allow access only to the owner of information and other authorized users or groups.

5.2.374. Carefully manage all interfaces.

5.2.375. Provide security levels for access to records and files.

5.2.376. Strictly control access enabling only privileged users or supervisors to override system controls or the capability of bypassing data validation on editing problems.

5.2.377. Restrict authority to change master files to persons independent of the data processing function.

5.2.378. Have access control mechanisms to prevent unauthorized access or changes to data, especially, the server file systems that are connected to the Internet, even behind a firewall.

5.2.379. Be capable of routinely monitoring the access to automated systems containing sensitive (as defined by County Policy) information.

5.2.380. Limit access to system utility programs to necessary individuals with specific designation.

5.2.381. Delete or disable all default accounts.

5.2.382. Restrict access to server file-system controls to ensure that all changes such as direct write, write access to system areas and software or service changes will be applied only through the appropriate change control process.

5.2.383. Restrict access to server-file-system controls that allow access to other users' files.

5.2.384. Ensure that servers containing user credentials will be physically protected, hardened and monitored to prevent inappropriate use.

5.3 Configuration and Change Management

5.3.1. Strict configuration management shall be followed, building a secure image that is used to build all new systems that are deployed to the enterprise.

5.3.2. Images shall be created for County devices including workstations, laptops, servers, routers, switches, etc. Images shall address security settings.

5.3.3. Any existing system that becomes compromised is re-imaged with the secure build.

Notes: Align with Incident Response processes. You do not want to re-image a device before its value has been leveraged.

5.3.4. Regular updates to this image are integrated into the organization's change management processes.

5.3.5. System images shall be tested before deployment including security settings to ensure that security settings do not adversely affect business operations.

5.3.6. Images shall be approved by a County designated change control board.

5.3.7. Documented images shall be registered with a central image library for the organization or multiple organizations.

5.3.8. These images shall be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors. When a production patch cycle is in process, the images shall be updated as well.

5.3.9. Standardized images shall represent hardened versions of the underlying operating system and the applications installed on the system.

5.3.10. This hardening would typically include removal of unnecessary accounts, disabling or removal of unnecessary services, configuring non-executable stacks and heaps, applying patches, closing open and unused network ports, implementing intrusion detection systems and/or intrusion prevention systems, and erecting host-based firewalls.

5.3.11. The master images themselves shall be stored on securely configured servers.

5.3.12. Such servers shall be monitored with integrity checking tools and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.

5.3.13. Images shall be tested at the hot or warm disaster recovery site.

Notes: Ensure alignment of the image lifecycle with Business Continuity/Disaster Recovery Planning.

5.3.14. Run the last version of software on the secure image and make sure it is fully patched. Remove outdated or older software from the system.

5.3.15. The latest stable version of any security-related updates shall be installed within 30 days of the update being released from the device vendor.

5.3.16. Any deviations from the standard build or updates to the standard build shall be approved by a change control board and documented in a change management system.

5.3.17. Negotiate contracts to buy systems configured securely out of the box using standardized images, which shall be devised to avoid extraneous software that would increase their attack surface and susceptibility to vulnerabilities.

5.3.18. Utilize application white listing to control and manage any configuration changes to the software running on the system.

5.3.19. All remote administration of servers, workstation, network devices, and similar equipment shall be done over secure channels.

5.3.20. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption shall only be used if they are performed over a secondary encryption channel, such as SSL or IPSEC.

5.3.21. Utilize file integrity checking tools on a daily basis to ensure that sensitive (as defined by County Policy) system files (including sensitive system and application executables, libraries, and configurations) have not been altered. Exceptions may be made on a per-system basis based on business needs.

5.3.22. All unauthorized alterations to such files shall be automatically reported to security personnel.

5.3.23. It might be that some level of criticality is applied to certain changes, such that the most critical unauthorized changes are reported immediately, others daily, and the least critical weekly.

5.3.24. The reporting system shall have the ability to account for routine and expected changes, highlighting unusual or unexpected alterations.

5.3.25. Implement an automated configuration monitoring system that measures all secure configuration elements that can be measured through remote testing, using features such as those included with tools compliant with Security Content Automation Protocol (SCAP) to gather configuration vulnerability information.

5.3.26. These automated tests shall analyze both hardware and software changes, network configuration changes, and any other modifications affecting security of the system.

Notes: In other words, you shall consider the breadth and depth of your systems when thinking about configuration settings. I like that the word “analyze” is included here, though it’s unclear if it really shall be. I would like to see configuration settings actually analyzed by assessment tools. To me, that means providing some additional context around the configuration setting when it’s not set according to the benchmark. Some tools do this today, though to a limited, text-based extent.

5.3.27. Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for Unix systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

5.3.28. Organizations need to adopt a formal process and management infrastructure for configuration control of mobile devices.

5.3.29. The process needs to include secure remote wiping of lost or stolen devices, approval of corporate apps, and denial of unapproved apps.

5.3.30. If the device is owned by the organization, a full wipe shall be performed.

5.3.31. If it is a BYOD system, a selective wipe shall be performed, removing the organization's information.

5.3.32. The Change Audit tool or System Monitoring tool shall be capable of identifying any changes to County devices, including workstations, laptops, servers, routers, switches, firewalls, and IDS and IPS systems. These changes include any modifications to key files, services, ports, configuration files, or any software installed on the device. Modifications include deletions, changes, or additions of new software to any part of the device configuration.

5.3.33. The configuration of each County device shall be checked against the official master image database to verify any changes to secure configurations that would impact security on a regular basis. This includes both operating system and configuration files.

5.3.34. File integrity checking tools shall be run on a regular basis.

5.3.35. Any changes to critical operating system, services, and configuration files shall be checked on an hourly basis.

5.3.36. System scanning tools that check for software version, patch levels, and configuration files shall be run on a monthly basis.

5.3.37. If possible, Change Audit tools or System Monitoring tools shall block installation, prevent execution, or quarantine unauthorized changes/software, alerting or sending e-mail when this action has occurred. Any unauthorized attempts to change a computer system shall be reported within 24 hours of detection. Notification performed by alerting or sending e-mail notification to a list of enterprise administrative personnel.

5.3.38. Any unauthorized changes detected on a device shall send a notification within 24 hours. Notification performed by alerting or sending e-mail notification to a list of enterprise personnel.

5.3.39. Every 24 hours after that point, the system shall alert or send e-mail about the status of the system until the system with the unauthorized change has been removed from the network or remediated.

5.3.40. Backups shall be made prior to making any changes to critical network devices.

5.3.41. It is critical that changes not impact or weaken the security of the device. Acceptable changes include but are not limited to making a comment or adding a duplicate entry in the configuration.

5.3.42. The change shall be performed twice for each critical device.

Secure Configurations for Network Devices

5.3.43. The standard security configuration of firewall, router, and switches shall be based on the Center for Internet Security and/or Defense Information Systems Agency.

5.3.44. Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization.

5.3.45. Any deviations from the standard configuration or updates to the standard configuration shall be documented and approved in a change control system.

5.3.46. Any network boundary moving from one security posture to another shall have ingress/egress filtering and be well controlled. For example, at network interconnection points, such as Internet gateways, inter-organization connections, and internal network segments with different security controls implement ingress and egress filtering to allow only those ports and protocols with an explicit and documented business need. All other ports and protocols shall be blocked with default-deny rules by firewalls, network-based IPS, and/or routers.

OR

Any network boundary moving from one security posture to another shall have ingress/egress filtering and be well-controlled.

5.3.47. All new configuration rules that allow traffic to flow through network security devices, such as firewalls and network-based IPS, shall be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.

5.3.48. Network filtering technologies employed between networks with different security levels (firewalls, network-based IPS tools, and routers with access controls lists) shall be deployed with capabilities to ensure network boundary scanning technology covers the specific network technologies in use.

5.3.49. Network devices shall be managed using two-factor authentication and encrypted sessions.

Secure Configurations for Network Ports, Protocols, and Services

5.3.50. Disable and uninstall all unnecessary services and components. Any installed service or component that is not needed shall be turned off for 30 days. After 30 days, the service or component shall be uninstalled from the system.

5.3.51. Host-based firewalls or port filtering tools shall be applied on end-user systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

Notes: Host-based filtering requires your organization to know what needs to be operated on these endpoints.

5.3.52. Automated port scans shall be performed on a regular basis against all key servers and compared to a known effective baseline.

5.3.53. If you scan and detect a deviation from your standard baseline for which you have no waiver, an alert shall be generated and reviewed.

5.3.54. All services shall be kept up to date.

5.3.55. Services needed for business use across the internal network shall be reviewed quarterly via a change control group, and business units shall re-justify the business use.

5.3.56. Services that are turned on for projects or limited engagements shall be turned off when they are no longer needed and properly documented.

5.3.57. Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.

Notes: If you are running critical services in VMs, then ensure you have some fail-over capability.

5.3.58. Application firewalls shall be placed in front of any critical servers to verify and validate the traffic going to the server.

5.3.59. Any unauthorized services or traffic shall be blocked and an alert generated.

Notes: You are going to have to have a way to tell the monitoring software what you consider to be authorized. Author your baseline standard once and have that propagate throughout your ecosystem?

5.3.60. In addition to determining which ports are open, effective port scanners shall be configured to identify the version of the protocol and service listening on each discovered open port.

5.3.61. The system shall be capable of identifying any new unauthorized listening network ports that are connected to the network within 24 hours, alerting or sending e-mail notification to a list of enterprise personnel.

Notes: You are going to want to integrate this system with your LDAP/AD system, so that you can take advantage of roles. Also, ensure that your system has some alerting mechanism, preferably one adapted for this domain.

5.3.62. Every 24 hours after that point, the system shall alert or send e-mail about the status of the system until the listening network port has been disabled or has been authorized by change management.

Notes: It would be interesting to collect metrics on how many nags are received before a problem/incident is corrected.

The system service baseline database and alerting system shall be able to identify the location, department, and other details about the system where authorized and unauthorized network ports are running.

5.4 Vulnerability Management

5.4.1. Run automated vulnerability scanning tools against all systems on their networks on a monthly or more frequent basis using a vulnerability scanner that looks for both code-based vulnerabilities (CVE) and configuration-based vulnerabilities (CCE).

5.4.2. Vulnerability scanning shall occur using an up-to-date vulnerability scanning tool. Signatures updated at least monthly.

5.4.3. Any vulnerability identified shall be remediated in a timely manner as follows:

- Critical vulnerabilities addressed within 30 calendar days
- High vulnerabilities addressed within 60 calendar days
- Medium vulnerabilities addressed within 90 calendar days

5.4.4. Event logs shall be correlated with information from vulnerability scans to fulfill two goals. First, personnel shall verify that the activity of the regular vulnerability scanning tools themselves is logged. Second, personnel shall be able to correlate attack detection events with earlier vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.

5.4.5. Utilize a dedicated account for authenticated vulnerability scans.

5.4.6. The scanning account shall not be used for any other administrative activities and tied to specific IP addresses.

5.4.7. Ensure only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.

5.4.8. Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures.

5.4.9. Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe.

5.4.10. “Patches shall be applied to all systems, even systems that are properly air gapped.”

5.4.11. Carefully monitor logs associated with any scanning activity and associated administrator accounts to ensure that all scanning activity and associated access via the privileged account is limited to the timeframes of legitimate scans.

5.4.12. Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk.

5.4.13. Such acceptance of business risks for existing vulnerabilities shall be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed increasing the risk.

5.4.14. Vulnerability scanning tools shall be tuned to compare services that are listening on each machine against a list of authorized services.

5.4.15. Measure the delay in patching new vulnerabilities and ensure that the delay is equal to or less than the benchmarks set forth by the organization.

5.4.16. Alternative countermeasures shall be employed if patches are not available.

5.4.17. Patches shall be evaluated in a test environment before being pushed into production on enterprise systems.

5.4.18. If such patches break critical business applications on test machines, the organization shall devise other mitigating controls that block exploitation on systems where the patch cannot be deployed because of its impact on business functionality.

5.4.19. Prioritize remediation of vulnerabilities based on the vulnerable assets using both the technical and organization-specific business risks.

5.4.20. To help standardize the definitions of discovered vulnerabilities in multiple departments of an organization or even across organizations, it is preferable to use vulnerability scanning tools that measure security flaws and map them to vulnerabilities and issues categorized using one or more of the following industry-recognized vulnerability, configuration, and platform classification schemes and languages: CVE, CCE, OVAL, CPE, CVSS, and/or XCCDF.

Notes: Results loaded into County GRC for management.

5.4.21. In addition to the scanning tools that check for vulnerabilities and misconfigurations across the network, various free and commercial tools can evaluate security settings and configurations of local machines on which they are installed. Such tools can provide fine-grained insight into unauthorized changes in configuration or the inadvertent introduction of security weaknesses by administrators.

5.4.22. Vulnerability scanners shall be linked with problem-ticketing systems that automatically monitor and report progress on fixing problems, and that make unmitigated critical vulnerabilities visible to higher levels of management to ensure the problems are solved.

5.4.23. Using County GRC software, compare the results of the current scan with previous scans to determine how the vulnerabilities in the environment have changed over time. Security personnel use these features to conduct vulnerability trending from month to month.

5.4.24. As vulnerabilities related to unpatched systems are discovered by scanning tools, security personnel shall determine and document the amount of time that elapses between the public release of a patch for the system and the occurrence of the vulnerability scan.

5.4.25. If this time window exceeds the organization's benchmarks for deployment of the given patch's criticality level, security personnel shall note the delay and determine if a deviation was formally documented for the system and its patch. If not, the security team shall work with management to improve the patching process.

5.4.26. All patch checks shall reconcile system patches with a list of patches each vendor has announced on its website.

5.4.27. All machines identified by the asset inventory system shall be scanned for vulnerabilities.

5.4.28. Additionally, if the vulnerability scanner identifies any devices not included in the asset inventory, it shall alert or send e-mail to enterprise administrative personnel within 24 hours.

5.4.29. Staff shall review to identify whether a scan was completed successfully.

5.4.30. Automated patch management tools shall alert or send e-mail to administrative personnel within 24 hours of the successful installation of new patches.

5.5 Cyber Incident Management

5.5.1. Each department shall have a written incident response plan that includes a definition of personnel roles for handling incidents. The procedures shall define the phases of incident handling.

5.5.2. Assign job titles and duties for handling computer and network incidents to specific individuals.

5.5.3. Define management personnel who will support the incident handling process by acting in key decision-making roles.

5.5.4. Incident Response Plan shall address standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that shall be included in the incident notification.

5.5.5. This reporting shall also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents.

5.5.6. Assemble and maintain information on third party contact information to be used to report a security incident (i.e., maintain an e-mail address of security@organization.com or have a web page http://organization.com/security).

5.5.7. Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team.

5.5.8. Such information shall be included in routine employee awareness activities.

5.5.9. Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.

5.6 Service Continuity Management

5.6.1. Each department shall have a written data restoration plan and Business Continuity Plan.

5.6.2. Each department shall ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive (as defined by County Policy) information.

5.6.3. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine shall each be included in the overall backup procedure.

5.6.4. All backup policies shall be compliant with any regulatory or official requirements.

5.6.5. Data on backup media shall be tested on a regular basis by performing a data restoration process to ensure that the backup is properly working.

5.6.6. Key personnel shall be trained on both the backup and restoration processes.

5.6.7. To be ready in case a major incident occurs, alternative personnel shall also be trained on the restoration process just in case the primary IT point of contact is not available.

5.6.8. Ensure that backups are properly protected via physical security or encryption when they are stored.

5.6.9. Ensure that backups are properly protected via physical security or encryption when they are moved across the network.

5.6.10. This includes remote backups and cloud services.

Notes: If your enterprise is using outsource providers for remote backup and/or cloud services, you need to determine whether their Information Security Program aligns with yours in this respect. This is not a technical problem in as much as it is an administrative one – you are going to have to spend some resources to validate, which shall always be included in cost of ongoing operations when considering such services.

5.6.11. Backup media, such as hard drives and tapes, shall be stored in physically secure, locked facilities.

5.6.12. End-of-life backup media shall be securely erased/destroyed.

5.6.13. Once per quarter (or whenever new backup equipment is purchased), a testing team shall evaluate a random sample of system backups by attempting to restore them on a test bed environment.

5.6.14. The restored systems shall be verified to ensure that the operating system, application, and data from the backup are all intact and functional.

5.7 Security Training and Awareness

5.7.1. Perform gap analysis to see which security areas employees are not adhering to and use this as the basis for an awareness program.

5.7.2. Organizations shall devise periodic security awareness assessments to be given to employees and contractors on at least an annual basis in order to determine whether they understand the information security policies and procedures, as well as their role in those procedures.

5.7.3. Develop security awareness training for various personnel job descriptions.

5.7.4. The training shall include specific, incident-based scenarios showing the threats an organization faces, and shall present proven defenses against the latest attack techniques.

5.7.5. Awareness shall be carefully validated with policies and training.

5.7.6. Awareness shall focus on the areas that are receiving the lowest compliance score.

5.7.7. Conduct periodic exercises to verify that employees and contractors are fulfilling their information security duties by conducting tests to see whether employees will click on a link from suspicious e-mail or provide sensitive (as defined by County Policy) information on the telephone without following appropriate procedures for authenticating a caller.

5.7.8. Provide awareness sessions for users who are not following policies after they have received appropriate training.

6 Processes

6.1 County Risk Management Process

The *Cybersecurity Best Practices Manual - Risk Management* domain (*Section 3.27* of this manual) provides guidance regarding the management of operational risks to IT-dependent critical services and the assets that support them. To effectively manage operational risk, organizations should establish processes (see Figure 1) to:

- identify risks to which the organization is exposed
- analyze risks and determine appropriate risk disposition
- control risks to reduce probability of occurrence and/or minimize impact
- monitor risks and responses to risks and improve the organization's capabilities for managing current and future risks

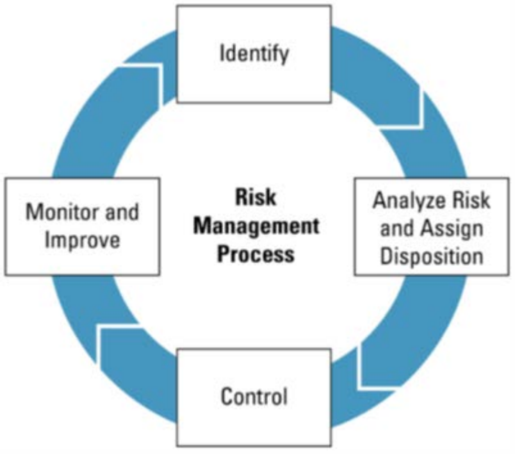


Figure 1: Overview of Risk Management Process

6.1.1 Identify risks

The identification of risks is a foundational risk management activity; an organization will have difficulty successfully managing its risks if it does not understand what they are. Organizations need to ensure they have the ability to identify risks in a timely manner and then communicate those risks to the appropriate stakeholders.

Identify the risks associated with the department's critical services and sensitive data (refer to *Section 3.2.1 - Asset Management* domain of this manual). Refer to *Appendix A: Section B.1 Identify Risks* of the *County Risk Management Process* (*Appendix M* of this manual) for more information.

Document each identified risk on a separate Risk Analysis and Disposition Worksheet:

Risk ID: Unique identifier assigned by department
Date: date worksheet completed
Risk Title: Brief summary of risk
Risk Description: Detailed description of risk
Risk Owner: Individual responsible for mitigating risk
Department:

Asset(s): assets impacted by risk
Critical Service: service impacted by risk
Actor:
Means:
Motive:
Outcome: Effect on asset if risk is realized

- Disclosure - information available to unauthorized persons
- Destruction - asset is permanently unavailable to the organization
- Interruption - asset is temporarily unavailable to the organization
- Modification - information was changed by an unauthorized person
- Other -

Security Requirements:
Existing Controls: Document existing controls to mitigate risk

- Maintain an inventory of the identified risks.

6.1.2 Analyze Risk and Assign Disposition

- Use the Risk Analysis and Disposition Worksheet to analyze each identified risk. Refer to *Appendix A: Section B.2 Analyze Risk and Assign Disposition* of *County Risk Management Process* (*Appendix M* of this manual) for more information.
- Assigning Priority for Impact Areas.
- This establishes the relative importance of each impact area to the department and should be used to support the risk analysis and disposition assignment activities. For example, the critical service may have regulatory requirements; therefore, “Compliance” would be assigned a higher priority than “Strategic - Reputation and Customer Confidence”. (Assign the lowest value to the highest priority.)

6.1.3 Assigning Impact of Risk

This establishes the impact of the risk to the identified services and assets. There should never be an expectation of no level of risk to information technology systems and data. Select the most appropriate impact:

- **High/Catastrophic** – Department loses all ability to use IT systems to serve the public and perform core business functions. The line of business supported by the system cannot be performed through technology mechanism. Department will have to consider utilizing analogue means of conducting the impacted line of business. (**Assign a value of 1**)
- **Medium/Moderate** – Department may still operate IT systems to serve the public and perform core business functions but on a degraded level and with delays in service to be expected. Quality of service is also likely to be impacted. Decisions may have to be made on limited the scope of services provided through impacted systems to support the line of business. The Line of business supported will be impacted at a level noticeable to the public. (**Assign a value of 2**)
- **Low /Impacted** – Department IT systems will continue to operate to serve the public and perform core business functions, but will system delays, sporadic outages and noticeable performance degradation will be characteristic of this level impact. Some functionality may be lost, but not enough to severely impede the line of business the systems support. This level of impact will not be noticeable to the public. (**Assign a value of 3**)

6.1.4 Assigning Likelihood of Risk

This establishes the likelihood of the risk occurring based on information received from intelligence sources, historical data and information provided by subject matter experts. Select the most appropriate likelihood:

- **High/Imminent** – Risk factor is will occur if mitigating controls are not in place. (**Assign a value of 1**)
- **Medium/Probable** – Risk factor is highly likely and under most conditions will occur. (**Assign a value of 2**)
- **Low/Plausible** – Risk factor is possible, but not likely. (**Assign a value of 3**)

6.1.5 Assign Disposition

Assigning a risk disposition defines the approach the department will use to manage the risk. Risk disposition assignment is a key risk management step that should be carefully undertaken with input from key internal and external stakeholders. The frequency (i.e., probability) of the realization of risk and the likely impact on the organization are key variables driving disposition decisions. Risk frequency and impact considerations are often combined with other strategic factors to inform disposition assignment. Because of the dynamic nature of today's risk–threat landscape, many organizations also utilize information provided by industry groups, governments, and vendors to support their disposition assignment and mitigation activities.

Select one of the following dispositions:

- **Accept**—an explicit or implicit decision not to take an action that would affect a particular risk.
- **Avoid**—a strategy or measure that effectively removes the exposure of an organization to a risk.
- **Control/Mitigate**—deliberate actions taken to reduce a risk's potential for harm or to maintain the risk at an acceptable level.
- **Defer/Monitor**—an explicit decision to further research and defer action on a risk until the need to address it is apparent and the risk is better understood.
- **Transfer**—shifting some or all of the risk to another entity, asset, system, network, or geographic area.

6.1.6 Acceptance of Risk

Acceptance of risk requires a formal memorandum kept on file with the documented risk assessment. To be considered valid, the risk acceptance must contain the following elements:

- Risk acceptance must be signed by the Department Head (This cannot be delegated).
- Risk acceptance must contain an acknowledgement of the risk (residual or unmitigated).
- The risk acceptance is submitted and approved via *County Variance Review & Approval Process.*

6.1.7 Controls

- Document control plans and recovery plans in the "Disposition Comments" section. For more information on developing and maintaining recovery plans refer to *Section 3.2.6 Service Continuity Management* of this manual.

- Communicate plans and status to stakeholders.

6.1.8 Monitor and Improve

Maintaining an effective operational risk program requires more than identifying risks, putting controls in place, and adding new controls over time. There must be a variety of supporting activities to monitor and improve the program. These activities include ensuring that the operational risk management processes are communicated and monitored for quality and effectiveness, and that coordination and collaboration with both internal and external stakeholders occur. Effective operational risk management can be seen as an iterative process improvement activity that requires frequent tuning and proactive collaboration to be successful.

Document risk monitoring strategy for the department that includes the purpose, type, and frequency of monitoring activities. Important activities in monitoring and improving risk management include the following:

- Track the status of existing, new, and potential future risks.
- Measure and report on risk mitigation efforts to determine if they are achieving the intended results by monitoring organizational information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes.
- Establish linkages to the organization’s other risk management activities (e.g., enterprise, credit, market, reputational).
- Coordinate and collaborate with external entities (e.g., regulators, service providers, business partners).

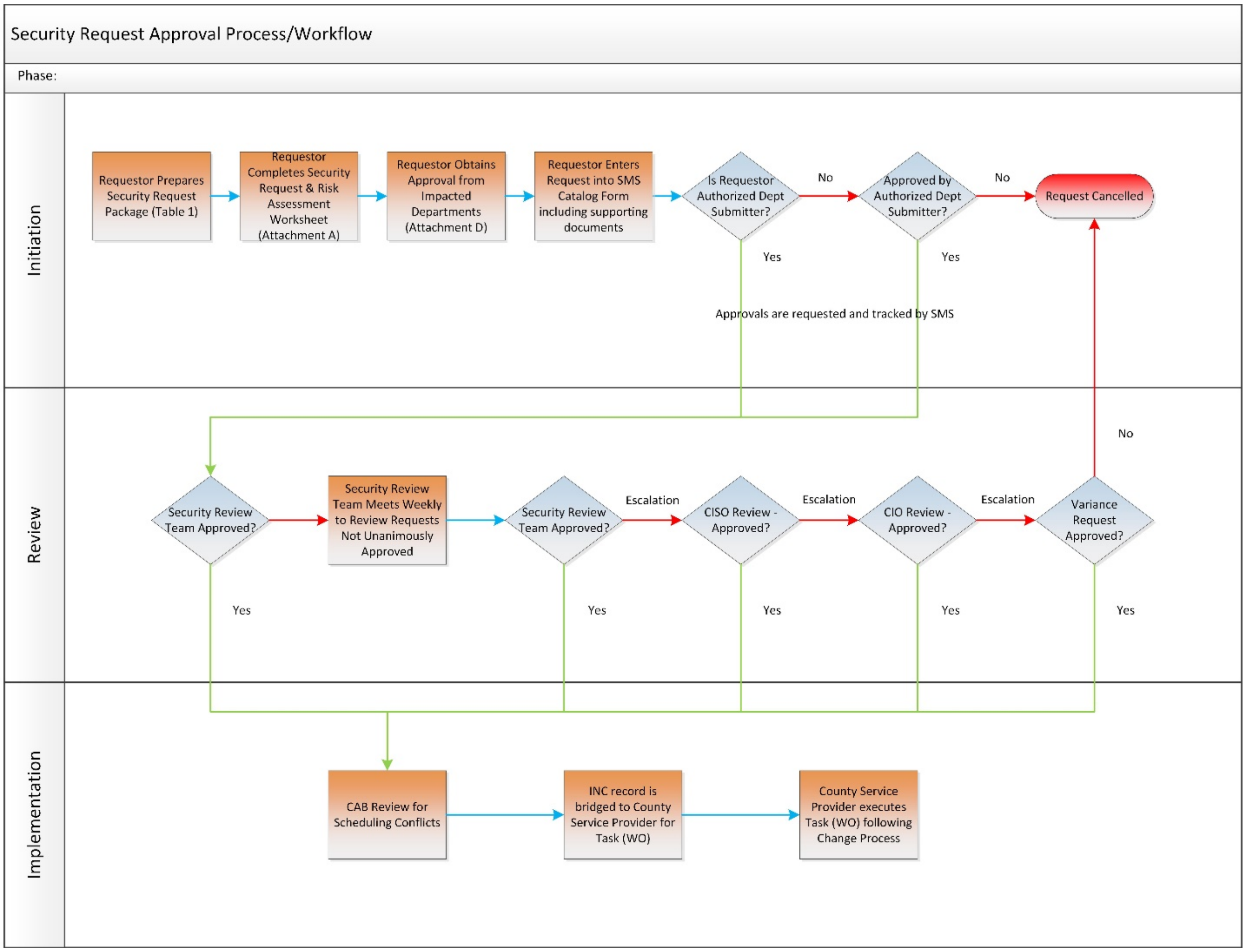
Each department shall conduct periodic risk assessments (at a minimum every three years) to ensure adequate cybersecurity controls exists to safe guard departmental information technology systems and data as measured against the risk tolerance for the department and the line of business. The risk assessment shall include the following:

- Date the risk assessment was conducted

Names of the individuals assigned to conduct the risk assessment.

To view the full document, visit link below.
https://ocgov.sharepoint.com/InfoCentral/KB/PPSG/policylib/Policy Best practices/County Risk Management Process.pdf

6.2 Security Review and Approval Process


Security Request Approval Process/Workflow
Phase:
Initiation
Requestor Prepares Security Request Package (Table 1)
Requestor Completes Security Request & Risk Assessment Worksheet (Attachment A)
Requestor Obtains Approval from Impacted Departments (Attachment D)
Requestor Enters Request into SMS Catalog Form including supporting documents
Is Requestor Authorized Dept Submitter?
No
Approved by Authorized Dept Submitter?
No
Request Cancelled
Yes
Yes
Approvals are requested and tracked by SMS
Review
No
Security Review Team Approved?
Security Review Team Meets Weekly to Review Requests Not Unanimously Approved
Security Review Team Approved?
Escalation
CISO Review - Approved?
Escalation
CIO Review - Approved?
Escalation
Variance Request Approved?
Yes
Yes
Yes
Yes
Yes
Implementation
CAB Review for Scheduling Conflicts
INC record is bridged to County Service Provider for Task (WO)
County Service Provider executes Task (WO) following Change Process

6.2.1 Prepare Request Package

- The security request package should be developed well in advance of the need. OCIT managed service provider has ten (10) business days to implement a change once approved.
- Requestor completes the submittal package (see *Table 1: Required Documentation by Request Type*).
- For requests that impact other departments, the requestor shall obtain documented approval from each impacted department prior to entering the request.
- If the department has questions filling out the documents, they can request assistance from OCIT managed service provider Service Desk and/or OCIT Enterprise Security in helping clarify any questions they have.
- New projects/solutions or changes to existing infrastructure shall have gone through the County's Architecture review process before beginning this process.

Table 1: Required Documentation by Request Type

Request Type	Required Documentation				
	Dept Risk Assessment (Appendix A)	F/W Spreadsheet (Appendix B)	Network Diagram (Appendix C)	Dept. Approval – if applicable	Error Message
Security Architecture	X		X	X	
Firewall	X	X	X	X	
Website Listing (Black/White) – BlueCoat	X			X	X
Application Listing (Black/White) - Cylance	X			X	X
Email Gateway	X			X	X
Administrator Accounts	X			X	

6.2.2 Prepare Risk Assessment

- Requestor completes the *Security Request and Risk Assessment Worksheet* including identification of potential risks from implementing the request, assets and services impacted by request, and impact evaluation. (Refer to *County Risk Management Process* for more information on completing impact analysis.)
- For requests that impact other departments, the requestor shall obtain documented approval from each impacted department.

6.2.3 Enter Security Request into Service Ticketing System

- The requestor enters the security request into service ticketing system attaching required supporting documentation as defined in *Table 1* above.
- If the requestor is not an approved SMS submitter, the system will forward request to departmental approver.
- Service ticketing system determines whether the submitted security request is complete. All necessary information is provided and all required documents are completed and attached to the security request.
- The completed review package will be retained in service ticketing system for reference and audit trail.

6.2.4 Security Team Review

- Security Review Team (see *Table 2* below for composition of team) reviews the submitted security request via the service ticketing system as received to determine whether risk from implementing the request is sufficiently mitigated.
- If the Security Review Team (unanimous approval) determines the risk is sufficiently mitigated, the request is approved and forwarded to the CAB, if applicable, otherwise the request is implemented using the approved Change Management Procedure.
- If any of the Security Review Team members have questions regarding the request or does not approve the request, the team members enter work notes to the ticket. Security Team members do not reject the ticket.

- Weekly, the Security Review Team will meet to review unapproved tickets. Requestor is invited to meeting to answer/clarify request.
- After the meeting, if one or more of the team members does not approve, the request is rejected and enters the escalation process.

Table 2: Security Review Team

Organization
Data Center and Service Desk Vendor Security Team
Network Vendor Security Team
OCIT Infrastructure
OCIT Enterprise Security
Business Relation Manager

6.2.5 Escalation Process

If the request is rejected by the Security Review Team, the request is automatically forwarded to the CISO for review.

- The CISO reviews the submitted security request to determine whether risk from implementing the request is sufficiently mitigated.
- If the CISO determines the risk is sufficiently mitigated, the request is approved and forwarded to the CAB, if applicable, otherwise the request is implemented using the approved Change Management Procedure.
- If the CISO determines the risk is not sufficiently mitigated or there are questions regarding the request, the request is rejected and returned to the requestor for clarification and modification.

If the request is rejected by the CISO, the request is automatically forwarded to the CIO for review.

- The CIO reviews the submitted security request to determine whether risk from implementing the request is sufficiently mitigated.
- If the CIO determines the risk is sufficiently mitigated, the request is approved and forwarded to the CAB, if applicable, otherwise the request is implemented using the approved Change Management Procedure.
- If the CIO determines the risk is not sufficiently mitigated or there are questions regarding the request, the request is rejected and returned to the requestor for clarification and modification.

If the department does not agree with the decision of the CIO, the department may complete and submit a variance request.

- The department completes and submits a variance request. Refer to *County Variance Review and Approval Process* for more information on the process.

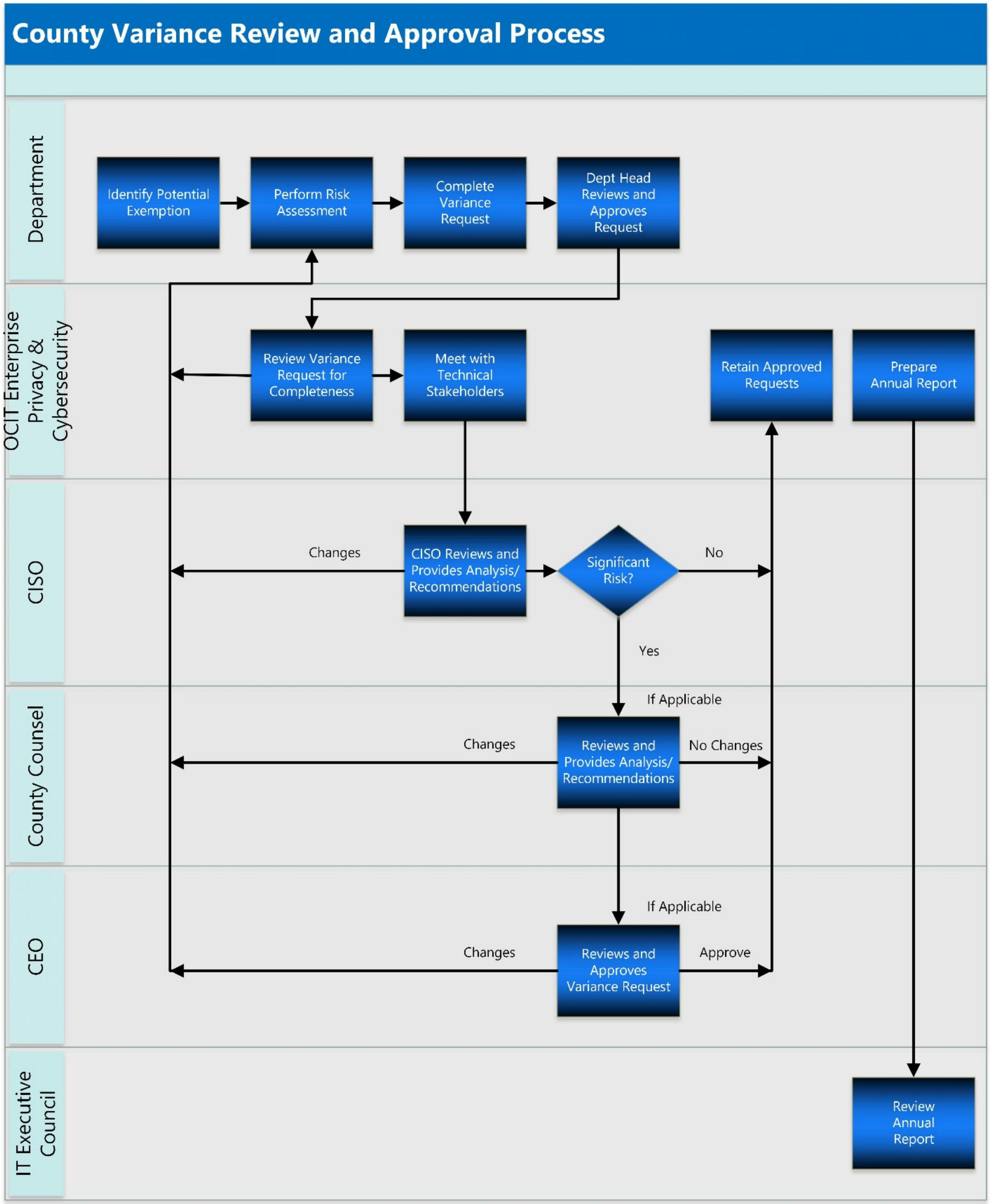
6.2.6 Change Advisory Board Review

- CAB reviews the submitted security request when it impacts multiple departments. CAB determines whether there are any issues or scheduling conflicts with implementing the request.

  If the CAB approves the request, it is forwarded to OCIT managed service provider for implementation using the approved Change Management Procedure.

  To view the full document, visit link below.
  https://ocgov.sharepoint.com/InfoCentral/KB/PPSG/policylib/County Policy Library/County Security Review and Approval Process Policy.pdf

6.3 County Variance Review and Approval Process


County Variance Review and Approval Process
Department
OCIT Enterprise Privacy & Cybersecurity
CISO
County Counsel
CEO
IT Executive Council
Identify Potential Exemption
Perform Risk Assessment
Complete Variance Request
Dept Head Reviews and Approves Request
Review Variance Request for Completeness
Meet with Technical Stakeholders
Retain Approved Requests
Prepare Annual Report
Changes
CISO Reviews and Provides Analysis/ Recommendations
Significant Risk?
No
Yes
If Applicable
Changes
Reviews and Provides Analysis/ Recommendations
No Changes
If Applicable
Changes
Reviews and Approves Variance Request
Approve
Review Annual Report

This process establishes best practices and the minimum requirements in order to maintain robust cybersecurity programs throughout the County's IT environment.

- Any request for variance from the Cybersecurity Best Practices Manual or County policy shall be reviewed in accordance with the criteria stated in Section 6.3.1 Variance Criteria, below, and the request for variance shall be documented using the County Variance Request Form.
- The request for variance shall be reviewed by a panel of qualified information security professionals. However, a request for variance that may involve, in the judgment of the CISO, sensitive, unique, or potentially significant risk to the department or County shall be reviewed by the CEO or designee. A significant risk to the department/agency or County shall be defined as any variance that affects another department in addition to the department requesting the variance or increases the potential for a breach of protected data.
- All requests for, and status of, any variance shall be logged in a central repository and accessible to all County staff involved in the submission or review of the County Variance Request Form.
- Approved County Variance Request Forms shall be reviewed at least annually for renewal by the CISO and the department requesting the variance.

6.3.1 Variance Criteria

- Requests shall be evaluated in the context of potential risk to the department and County as a whole.
- Request evaluations shall take into account what value the variance will bring to the department requesting the variance.
- Requests without compensating measures will not be accepted.
- Requests shall be consistently evaluated in accordance with County's risk acceptance practice.

6.3.2 Mitigation Criteria

- Mitigation measures shall minimize the County's net security risk resulting from variances from the Cybersecurity Best Practices Manual.

6.3.3 Prepare Variance Request Package

- If a department determines that they are unable to comply with a requirement of the Cybersecurity Best Practices Manual and/or County policy, the department shall evaluate whether to request a variance from the Cybersecurity Best Practices Manual and/or County policy. The department shall consider what risks they may face by not adhering to the best practice and/or policy as well as the benefit(s) gained by requesting the risk mitigation.
- The department shall complete the County Variance Request Form including the requirement not being met, risks associated with non-compliance, defining the proposed mitigation actions, and identifying the benefit of allowing the variance.
- Department Head approves the County Variance Request Form. In so doing, the department is accepting the potential risk caused by allowing the variance.
- Once OCIT Enterprise Privacy and Cybersecurity receives the County Variance Request Form, they shall log the form, review the submission for completeness (ensure no information is missing), and follow up with the department as necessary.

- OCIT Enterprise Privacy and Cybersecurity shall determine whether risk mitigation measures affect any other departments and work with the other departments to assess the impact of the risk mitigation measures to the other departments.
- OCIT Enterprise Privacy and Cybersecurity, Departmental Information Security Officer (DISO) and department’s technical stakeholder shall meet, as deemed necessary, to review the County Variance Request Forms. The purpose of the review is to examine the request, and discuss the potential risk and proposed mitigation by the department. OCIT Enterprise Privacy and Cybersecurity shall work with the department to understand the reason for the variance and propose reasonable alternatives to both mitigate the risk as well as provide the necessary functionality needed by the Department.
- CISO reviews the form and provides a recommendation.
- When appropriate, the CISO shall inform the Department Head, CEO, and CIO of the variance request regarding the risks and mitigation measures.
- When appropriate, CEO or designee reviews and approves the County Variance Request Form. Requests involving sensitive, unique, or potentially significant risk situations shall be reviewed by the CEO or designee.
- An electronic copy of the County Variance Request Form shall be maintained by OCIT Enterprise Privacy and Cybersecurity.
- Annually, OCIT Enterprise Privacy and Cybersecurity shall provide a report to the IT Executive Council listing the approved County Variance Request Forms including risk, mitigation measures, department, and reason for risk mitigation.
- The approval shall be in effect for a period of no more than one year from the time the variance is granted. At the end of the year, the variance and mitigation measures shall be reviewed and either terminated or renewed for another period not to exceed one year.
- When there is a change of Department Head, the incoming Department Head may review the approved County Variance Request Form(s) and determine whether to keep or terminate each variance.

To view the full document, visit link below.
https://ocgov.sharepoint.com/InfoCentral/KB/PPSG/policylib/County Policy Library/County Variance Review and Approval Process Policy.pdf

7 County Plans

7.1 County Cyber Incident Response Plan

7.1.1 Cyber Incident Management Lifecycle

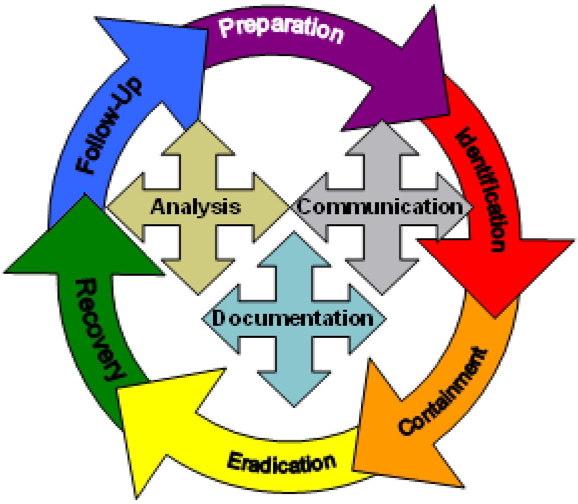


Figure 7.1 – The Cyber Incident Management Lifecycle

Cyber Incident Management in Orange County is a lifecycle approach, represented by Figure 7.1 – The Cyber Incident Management Lifecycle, and is composed of serial phases (Preparation, Identification, Containment, Eradication, Recovery, and Follow-Up) and of ongoing parallel activities (Analysis, Communication, and Documentation). This lifecycle is derived from many standardized cyber incident response processes such as those published by National Institute of Standards and Technology (NIST) and other authorities. The following are descriptions of those actions that comprise Orange County's Cyber Incident Management Lifecycle:

- **Preparation:** Maintaining and improving cyber incident response capabilities;
- **Identification:** Confirming, categorizing, scoping, and prioritizing suspected cyber incidents;
- **Containment:** Minimizing loss, theft of information, or service disruption;
- **Eradication:** Eliminating the threat;
- **Recovery:** Restoring computing services quickly and securely; and
- **Follow-Up:** Assessing response to better handle future incidents through utilization of reports, "Lessons Learned" and after-action activities, or mitigation of exploited weaknesses to prevent similar incidents from occurring in the future.

Cross-Cutting elements present throughout the Cyber Incident Management Lifecycle:

- **Communication:** Notifying appropriate internal and external parties and maintaining situational awareness;
- **Analysis:** Examining available data to support decision-making throughout the Cyber Incident Management Lifecycle; and

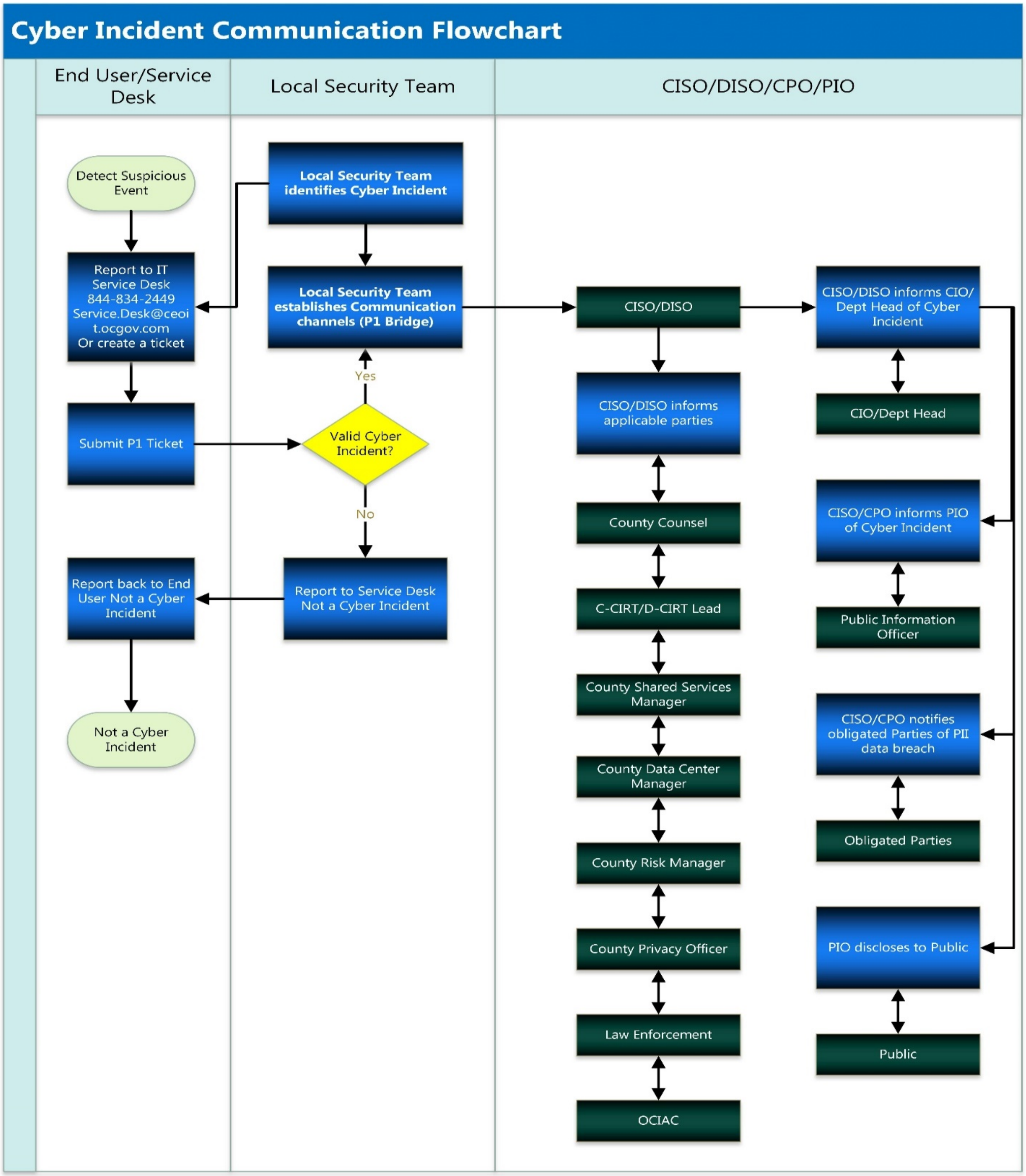
- **Documentation:** Recording and time-stamping all evidence discovered, information, and actions taken from Identification through Follow-Up.

7.1.2 Cyber Incident Communication Flow

Cyber Incident communication flows as represented by Figure 7.1.2 – Cyber Incident Communication Flowchart, and is composed of several steps (some of which are performed in parallel):

1. End User detects suspicious event such as phishing email, unusually sluggish computer, malware/ransomware warning, or unusual computer activity and reports it to Central IT Service Desk.
2. Service Desk assigns P1 ticket to Local Security Team. Service Desk does not research incident.
3. Local Security Team notifies CISO within 1 hour of learning of cyber incident.
4. Local Security Team determines (within 24 hours) whether valid cyber incident and communicates determination to service desk to advise End User.
5. Local Security Team opens conference bridge (P1 bridge).
6. Local Security Team reports incident to CISO and applicable DISO within one (1) hour of determination.
7. CISO notifies DISO, County Counsel, County Risk Manager, County Privacy Officer, C-CIRT/D-CIRT, County Shared Services Manager, County Data Center Manager, Law Enforcement, OCIAC, as appropriate, to coordinate investigation, analysis, and plans of action.
8. CISO notifies CIO, CEO, and Board of Supervisors using the email account according to the County's Significant Incident/Claim Reporting Protocol to brief them on the cybersecurity incident.
9. DISO notifies Dept. Head.
10. DISO (coordinating with County Privacy Officer) notifies PIO and obligated third parties when there is a potential data breach of PII. Refer to Section 7 – Related Documents of *Cyber Incident Response Plan* for more information on disclosure requirements per applicable rules, laws, and regulations.
11. Local Security Team/C-CIRT/D-CIRT reports status to CISO/DISO. Refer to Section 3.8.d – Status Reports of *Cyber Incident Response Plan* for more information
12. DISO reports status to Dept. Head. CISO provides status reports to CIO. Refer to Section 3.8.d – Status Reports of *Cyber Incident Response Plan* for more information
13. Local Security Team/C-CIRT/D-CIRT provides post-incident report. Refer to Section 3.7 c – Post Cyber Incident Report of *Cyber Incident Response Plan* for more information
14. PIO discloses incident to public when applicable. Refer to Section 3.8.e – Public Disclosure of *Cyber Incident Response Plan* for more information.
15. Annually, County departments shall review and confirm the accuracy of the Annual Confirmed Cybersecurity Incident(s) Report prepared by the County Enterprise Privacy and Cybersecurity Team. Departments shall return the report to the CISO with corrections or confirmation of its accuracy within one business week of receiving the report.

Figure 7.1.2: Cyber Incident Communication Flowchart


Cyber Incident Communication Flowchart
End User/Service Desk
Local Security Team
CISO/DISO/CPO/PIO
Detect Suspicious Event
Report to IT Service Desk 844-834-2449 Service.Desk@ceoit.ocgov.com Or create a ticket
Submit P1 Ticket
Report back to End User Not a Cyber Incident
Not a Cyber Incident
Local Security Team identifies Cyber Incident
Local Security Team establishes Communication channels (P1 Bridge)
Yes
Valid Cyber Incident?
No
Report to Service Desk Not a Cyber Incident
CISO/DISO
CISO/DISO informs applicable parties
County Counsel
C-CIRT/D-CIRT Lead
County Shared Services Manager
County Data Center Manager
County Risk Manager
County Privacy Officer
Law Enforcement
OCIAC
CISO/DISO informs CIO/ Dept Head of Cyber Incident
CIO/Dept Head
CISO/CPO informs PIO of Cyber Incident
Public Information Officer
CISO/CPO notifies obligated Parties of PII data breach
Obligated Parties
PIO discloses to Public
Public

To view the full document, visit link below.
https://ocgov.sharepoint.com/InfoCentral/KB/PPSG/policylib/Policy Best practices/Cyber Incident Response Plan.pdf

7.2 County Business Continuity Policy

Placeholder for link to County Business Continuity Policy (being revised)

8 References

Document	Issued By
County Risk Management Process (https://ocgov.sharepoint.com/InfoCentral/KB/PPSG/policylib/Policy Best practices/County Risk Management Process.pdf)	County of Orange
County Variance Review and Approval Process (https://ocgov.sharepoint.com/InfoCentral/KB/PPSG/policylib/County Policy Library/County Variance Review and Approval Process Policy.pdf)	County of Orange
County Security Review and Approval Process (https://ocgov.sharepoint.com/InfoCentral/KB/PPSG/policylib/County Policy Library/County Security Review and Approval Process Policy.pdf)	County of Orange
County Cyber Incident Response Plan (https://ocgov.sharepoint.com/InfoCentral/KB/PPSG/policylib/Policy Best practices/Cyber Incident Response Plan.pdf)	County of Orange
Department of Homeland Security Cyber Resilience Review (https://www.us-cert.gov/ccubedvp/assessments)	Department of Homeland Security
CRR Supplemental Resource Guide – Asset Management (https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-AM.pdf)	Department of Homeland Security
CRR Supplemental Resource Guide – Controls Management (https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-CM.pdf)	Department of Homeland Security
CRR Supplemental Resource Guide – Configuration & Change Management (https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-CCM.pdf)	Department of Homeland Security
CRR Supplemental Resource Guide – Vulnerability Management (https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-VM.pdf)	Department of Homeland Security
CRR Supplemental Resource Guide – Incident Management (https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-IM.pdf)	Department of Homeland Security
CRR Supplemental Resource Guide – Service Continuity Management (https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-SC.pdf)	Department of Homeland Security
CRR Supplemental Resource Guide – Risk Management (https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-RM.pdf)	Department of Homeland Security

Document	Issued By
CRR Supplemental Resource Guide – External Dependencies Management (https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-EDM.pdf)	Department of Homeland Security
CRR Supplemental Resource Guide – Training & Awareness (https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-TA.pdf)	Department of Homeland Security
CRR Supplemental Resource Guide – Situational Awareness (https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-SA.pdf)	Department of Homeland Security
CERT Resilience Management Model (http://www.cert.org/resilience/rmm.html)	Carnegie Mellon University's Software Engineering Institute

9 Cybersecurity Glossary of Terms

Administrative Account: Also referred to as privileged, supervisor, administrator, admin, or root access, administrative accounts provide greater permissions to resources than a normal user.

Antivirus/Anti-malware software: A program that monitors a computer or network to identify all types of malware and prevent or contain malware incidents.

Asset: In computer security, a major application, general-support system, high-impact program, physical plant, mission-critical system, personnel, equipment, or a logically related group of systems.

Attack Vector: A path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

Authentication: The process of verifying the identity of an individual user, machine, software component, or any other entity.

Baseline configuration: A set of specifications for a system, or configuration item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and that can be changed only through change-control procedures. The baseline configuration is used as a basis for future builds, releases, or changes.

Baselining: the act of implementing or returning a system to a baseline configuration.

Bogon: a bogus IP address from the bogon space, which is a set of IP addresses not yet officially assigned to any entity by the Internet Assigned Number Authority (IANA) or a regional Internet registration institute. Bogon IP addresses are legitimate addresses.

Border router: A device located at the organization’s boundary to an external network.

Business continuity: The ability to maintain operations and services—both technology and business—in the event of a disruption to normal operations and services. Ensures that any impact or disruption of services is within a documented and acceptable recovery period and that system or operation are resumed at a documented and acceptable point in the processing cycle.

Cell phone: Any mobile devise that can be connected to a cellular network regardless of make or model. Synonymous with mobile phone.

Common Vulnerabilities and Exposures (CVE): Listing of publicly known information security vulnerabilities and exposures operated and maintained by the Mitre Corporation. The listing is available at http://cve.mitre.org/cve/

Confidential data: Sensitive information intended for limited business use may be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of Department employees, clients, partners, or member of the public. Information in this category may be accessed and used by internal parties only when specifically authorized to do so in the performance of their duties. External parties requesting this information for authorized Department business must be under contractual obligation of confidentiality with the Department. The Department shall follow its disclosure policies and procedures before providing this information to external parties. Refer to Data Information Classification & Handling Policy for more information.

Confidentiality/Non-Disclosure Agreement: An agreement that outlines sensitive materials or knowledge two or more parties wish to share with one another. By way of such agreement, the parties to the agreement agree not to share or discuss with outside parties the information covered by the agreement.

County Enterprise Network: The electronic infrastructure components within the County allowing the departments to communicate with each other and the internet including backbone network, wide area networks (WAN), wireless local area network (Wi-Fi), radio frequency identification (RFID), bridges, switches, routers and firewalls.

Information Technology Systems: Also known as IT systems, include but are not limited to, county owned computers, servers, networks, network share drives, e-mail systems, laptops, cell phones and tablets. Each department is responsible for operation and maintenance of their devices. Departments may participate in OCIT Shared Services for these services.

Critical system [infrastructure]: The systems and assets, whether physical or virtual, that is so vital that the incapacity or destruction of such may have a debilitating impact.

Cyber-attack: Attempts to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network. An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber incident: A past, ongoing, or threatened intrusion, disruption, or other event that impairs or is likely to impair the confidentiality, integrity, or availability of electronic information, information systems, services, or networks.

Cybersecurity: The protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

Data: Any information created, sent, stored, or received on an information technology system. Data can be, but not limited to, files, documents, spreadsheets, videos, e-mails, presentations, pictures, videos, or music.

Data at Rest: Generally refers to data stored in persistent storage such as on a hard drive, CD/DVD, thumb drive or tape. It is archived data or data that is not accessed nor is moving through networks.

Data Classification (Policy): Orange County's policy used to categorize data to convey required safeguards for information confidentiality, integrity, and availability; establishes controls required based on value and level of sensitivity.

Data in Transit: The process of the transfer of data between all the versions of the original file especially when data is in transit on the internet.

Database: A collection of data that is stored on any type of computer storage medium and may be used for more than one purpose.

Data loss prevention (DLP): A comprehensive approach (covering people, processes, and systems) of implementing policies and controls designed specifically to discover, monitor, and protect confidential data wherever it is stored, used, or in transit over the network and at the perimeter.

Demilitarized Zone (DMZ): a section of a network that exists between the intranet and a public network, such as the Internet. It may contain a single host or multiple computer systems.

Department: A County entity, and all of its respective employees, volunteers, vendors, officers, departments, bureaus and institutions.

Disaster Recovery (Plan): A plan that describes the process to recover from major processing interruptions.

Distributed denial of service (DDoS): A type of attack that makes a computer resource or resources unavailable to its intended users. Although the means to carry out, motives for, and targets of a DDoS attack may vary, it generally consists of the concerted efforts of a group that intends to affect an institution's reputation by preventing an Internet site, service, or application from functioning efficiently.

Documents: Microsoft Office and Adobe Portable Document Format have native encryption features that supports algorithm up to 128 bits.

Domain: Microsoft network system consisting of the laptops, desktops and servers that control access to the County and County entity provided networks. Internet access, access to County e-mail, and mobile devices access is controlled by the domain.

Domain: A collection of related security objectives or controls identified by its central topic such as asset management, controls management, change & configuration management, etc. In the Cyber Resilience Review.

Elevated Permission Accounts: These are user accounts for domain and systems administrators. They allow the owner of the account a higher level of control and access to network software, hardware, computers and servers. Personnel that may possess these accounts will work in network operations, network security or the help desk.

e-Protected Health Information (e-PHI): any individual identifiable health information that is transmitted by electronic media or maintained in electronic media.

E-mail: E-mail systems can support Transport Layer Security (TLS) or S/MIME.

Encryption: A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that data appears as meaningless strings of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.

Enterprise network: The configuration of computer systems within an organization. Includes local area networks (LAN), wide area networks (WAN), bridges, and applications.

Enterprise-wide: The entire organization, rather than a single Department, Agency or unit.

Exploit: A technique or code that uses a vulnerability to provide system access to the attacker. An exploit is an intentional attack to impact an operating system or application program.

External connections: An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

FTP (file transfer protocol): A standard high-level protocol for transferring files from one computer to another, usually implemented as an application level program.

Firewall: Hardware or software link in a network that relays only data packets clearly intended and authorized to reach the other side.

Information System: Also known as IT systems, include but are not limited to, county owned computers, servers, networks, network share drives, e-mail systems, laptops, cell phones and tablets. Each department is responsible for operation and maintenance of their devices. Departments may participate in OCIT Shared Services for these services.

Intrusion Detection System/Intrusion Prevention System (IDS/IPS): A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its target.

"Jail-Break" or "Rooted": Terms used to describe a mobile device which has removed the software restrictions imposed by the device vendor allowing root access to the iOS. This in turn allows the downloading and installation of additional applications, extensions, and themes that are not available through the official vendor app store. This is accomplished by using a series of software exploits.

Jumpbox: Jumpbox or Jump servers are typically placed between a secure zone and the systems to be managed, such as a DMZ, to provide transparent management once a management session has been established. These types of servers function as a single audit point for traffic and user accounts.

Local User Accounts: Local accounts are user accounts used to access standalone systems, hardware, specialized software or other devices that require a user logon to manage or use.

Malware: Designed to secretly access a computer system without the owner's informed consent. The expression is a general term (short for malicious software) used to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, ransomware, crimeware, most rootkits, and other malicious and unwanted software or programs.

Metrics: A quantitative measurement.

Mobile device: A portable computing and communications device with information-storage capability. Examples include notebook and laptop computers, cellular telephones and smart phones, tablets, digital cameras, and audio recording devices.

Mobile Device Management Suite: A centralized technology that can enforce enterprise security policies on the mobile device. Application is installed on the mobile device to allow the County to manage the device including configuration and usage monitoring.

National Institute of Standards and Technology (NIST): An agency of the U.S. Department of Commerce that works to develop and apply technology, measurements, and standards; developed a voluntary cybersecurity framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructures.

Network: Two or more computer systems grouped together to share information, software, and hardware.

Network Appliance: A type of computing appliance that aids in the flow of information to other network-connected computing devices. Services that may be provided by a network appliance include firewall functions, caching, authentication, network address translation and IP address management.

Non-County Employee: Any individual performing work for the County of Orange who is not a county employee. This may include, but is not limited to, a contractor, intern, volunteer, vendor, etc., who is not a direct employee of the County.

Official Use Data: Potentially sensitive information not protected from public disclosure but if made easily and readily available may jeopardize the privacy or security of Department employees, clients, or partners. The Department shall follow its disclosure policies and procedures before providing this information to external parties.

On-boarding/Off-boarding

Patch and Vulnerability Management: the process for identifying, acquiring, installing, and verifying patches for products and systems to eliminate vulnerabilities, significantly reduce the opportunities for exploitation and add new features to software and firmware, including security capabilities

Peripheral Component Interconnect (PCI): a standard for connecting computers and their peripherals

Personally Identifiable Information (PII): Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Portable Device: see Mobile Device.

Posting: Writing, placing pictures or uploading data on a shared internet/intranet social media accounts, blogs, forums, etc.

Protected Health Information: Any individual identifiable health information that is created, transmitted, or maintained by a covered entity in any form or medium.

Public Key Infrastructure (PKI): A PKI enables users of an unsecured public network such as the internet to securely and privately exchange data through the usage of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

Public Wi-Fi: Network access provided to the public. Public Wi-Fi networks are unsecure and can easily allow nefarious actors to capture login credentials, encryption keys, and access to County networks. County offers Public Wi-Fi in its buildings via the "OC-Public" network.

Published Data: Low sensitive information. Information not protected from disclosure and, if disclosed, will not jeopardize the privacy or security of Department employees, clients, or partners. This includes information regularly made available to the public via electronic, verbal, or hard copy media. Refer to Data Information Classification & Handling Policy for more information.

Radio Frequency Identification (RFID): A radio-frequency identification system uses *tags*, or *labels* attached to the objects to be identified. Two-way radio transmitter-receivers called *interrogators* or *readers* send a signal to the tag and read its response.

Removable media: Portable electronic storage media, such as magnetic, optical, and solid-state devices, which can be inserted into and removed from a computing device and which is used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and similar storage devices.

Removable Media: Any type of storage device that can be removed from a computer with the system is running. For example: CD's, DVD's, USB drives.

Risk assessment: A prioritization of potential business disruptions based on severity and likelihood of occurrence. The risk assessment includes an analysis of threats based on the impact to the institution, its customers, and financial markets, rather than the nature of the threat.

Router: A hardware device that connects two or more networks and routes incoming data packets to the appropriate network.

Secure Socket Layer (SSL): Uses a public key cryptography to encrypt Web Application session between the Web server and user's browser. The web server must have a certificate that has been generated by a Public Key (PKI) and the user's browser comes pre-configured to "trust" the certificates of these well-known CA's.

Security log: A record that contains login and logout activity and other security-related events and that is used to track security-related information on a computer system.

Security posture: The security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, and policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

Security Technical Implementation Guide (STIG): A Security Technical Implementation Guide (STIG) is a cybersecurity methodology for standardizing security protocols within networks, servers, computers, and logical designs that enhance overall security. These guides, when implemented, enhance security for software, hardware, physical and logical architectures to further reduce vulnerabilities.

Server: A computer or other device that manages a network service. An example is a print server, which is a device that manages network printing.

Service Accounts: These are specialized user accounts that enable systems to gain access to the domain and are not used by a user or administrator on the network. Service accounts are used by software and hardware appliances to login to the domain in order for the specialized software or hardware to provide services to County IT systems users. Service accounts may also be required by software and devices to allow an application, service or hardware to function.

Social engineering: A general term for trying to trick people into revealing confidential information or performing certain actions.

Spear phishing: An attack targeting a specific user or group of users, and attempts to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link. Spear phishers rely on knowing some personal piece of information about their target, such as an event, interest, travel plans, or current issues. Sometimes this information is gathered by hacking into the targeted network.

System: A system refers to a specialized server and/or piece of software that performs a specific business requirement which may or may not require a user name and password to access. A system by this definition is not considered the same as the Domain. Users can have domain access without having a particular system access.

System administrator: An individual responsible for the installation, management, and control of a network.

Transmitting: Sending information over an electronic medium such as e-mail, instant messaging, uploading documents to social media accounts, blogs, forums, file transfer sites, etc.

User: Anyone, to include employees, elected officials, temporary help, contractors, vendors or volunteers who has been granted access to County Information Technology Systems.

Virtual Local Area Network (VLAN): is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic.

Virtual Private Network (VPN): Uses software or hardware to encrypt data between clients and networks. IP Security (IPSec) provides authentication between sites. IPSec authentication is an exchange of keys between communicating devices.

Wireless Local Area Networking (Wi-Fi): Wi-Fi compatible devices can connect to the network via a WLAN network and a wireless access point. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometers achieved by using multiple overlapping access points.

10 Acronyms

AD: Active Directory

AV: Anti-Virus Software

C-CIRM: County Cyber Incident Response Manager

C-CIRT: County Cyber Incident Response Team

CIM: Cyber Incident Management

CIO: Chief Information Officer

CIRM: Cyber Incident Response Manager

CIRT: Cyber Incident Response Team

CISO: Center Chief Information Security Officer

CoCo: County Counsel

CPO: County Privacy Officer

CTG: Computer Task Group

CVE: Common Vulnerabilities and Exposures

D-CIRM: Department Cyber Incident Response Manager

D-CIRT: Department Cyber Incident Response Team

DHCP: Dynamic Host Configuration Protocol

DISO: Department Information Security Officer (for a specific department)

DDoS: Distributed Denial of Service

DMZ: Demilitarized Zone

DoS: Denial of Service

FA: Forensic Analyst

FIPS: Federal Information Processing Standards

IDS/IPS: Intrusion Detection System/Intrusion Prevention System

ISO: Information Security Officer (Managed Services/Shared Services)

LDAP: Lightweight Directory Access Protocol/Active Directory

NIA: Network Incident Analyst

NIST: National Institute of Standards and Technology

OCIAC: Orange County Intelligence Assessment Center

OCIT: Orange County Information Technology

OCSD: Orange County Sheriff's Department

OS: Operating System

PCI: Peripheral Component Interconnect

PII: Personally Identifiable Information

PIO: Public Information Officer (County or a specific department)

RACI: Responsible, Accountable, Consulted, and Informed

RFID: Radio Frequency Identification

SDM: Service Delivery Manager

SME: Subject Matter Expert

STIG: Security Technical Implementation Guide

TI: Technical Investigator

US-CERT: United States-Computer Emergency Readiness Team

VLAN: Virtual Local Area Network

VM: Virtual Machine

Appendix A – Asset Management Controls

Cyber Resilience Review Goals and Practices – Asset Management (AM)

In order for an asset management process to be considered valid and complete, at a minimum, the following objectives shall be addressed:

AM.1 Services are identified and prioritized including:

- Services are identified.
- Services are prioritized based on analysis of the potential impact if the services are disrupted.

AM.2 Assets are inventoried, and the authority and responsibility for these assets is established including:

- The assets that directly support the critical service are inventoried (technology includes hardware, software, and external information systems).
- Asset descriptions include protection and sustainment requirements.
- Both owners and custodians of assets are documented in asset descriptions.
- The physical location of assets (both within and outside the organization) are documented in the asset inventory.

AM.3 The relationship between assets and the services they support is established including:

- The associations between assets and the critical service they support are documented.
- Confidentiality, integrity, and availability requirements are established for each service-related asset.

AM.4 The asset inventory is managed including:

- Change criteria have been established for asset descriptions.
- Asset descriptions are updated when changes to assets occur.

AM.5 Access to assets is managed including:

- Access (including identities and credentials) to assets is granted based on their protection requirements.
- Access (including identities and credentials) requests are reviewed and approved by the asset owner.
- Access privileges are reviewed to identify excessive or inappropriate privileges.
- Access privileges are modified as a result of reviews.

AM.6 Information assets are categorized and managed to ensure the sustainment and protection of the critical service including:

- Information assets are categorized based on sensitivity and potential impact to the critical service (such as published, official use, or confidential).

- The categorization of information assets is monitored and enforced.
- There are policies and procedures for the proper labeling and handling of information assets.
- All staff members who handle information assets (including those who are external to the organization, such as contractors) are trained in the use of information categories.
- High-value information assets are backed up and retained.
- Guidelines exist for properly disposing of information assets.
- Adherence to information asset disposal guidelines is monitored and enforced.

AM.7 Facility assets supporting the critical service are prioritized and managed including:

- Facilities are prioritized based on potential impact to the critical service, to identify those that should be the focus of protection and sustainment activities.
- The prioritization of facilities is reviewed and validated.
- Protection and sustainment requirements of the critical service are considered during the selection of facilities.

Refer to CRR Supplemental Resource Guide – Asset Management and CERT Resilience Management Model for additional guidance on asset management process.

See Appendix L – Controls Crosswalk for correlation of Cybersecurity Program controls with NIST 800-53 r4.

Appendix B – Controls Management Controls

Cyber Resilience Review Goals and Practices – Controls Management (CM)

In order for a controls management process to be considered valid and complete, at a minimum, the following objectives shall be addressed:

CM.1 Control objectives are established including:

- Control objectives have been established for assets required for delivery of the critical service.
- Control objectives are prioritized according to their potential to affect the critical service.

CM.2 Controls are implemented including:

- Controls have been implemented to achieve the control objectives established for the critical service.
- Controls have been implemented for the following:
  - Network Segregation
  - Data at Rest
  - Data in Transit
  - Data Leaks
  - Audit/Record Logs
  - Removable Media
  - Communication and Control Networks
  - Human Resource Practices
  - Access to systems and assets controlled based on principle of least functionality

Refer to Administrative Controls, Technical Controls, and Processes sections for complete listing of control requirements.

CM.3 Control designs are analyzed to ensure they satisfy control objectives including:

- Control designs are analyzed to identify gaps where control objectives are not adequately satisfied.
- As a result of the controls analysis, new controls are introduced or existing controls modified to address gaps.

CM.4 Internal control system is assessed to ensure control objectives are met including:

- The performance of controls is assessed on a scheduled basis to verify they continue to meet control objectives.
- As a result of scheduled assessments, new controls are introduced or existing controls modified to address problem areas.

Refer to CRR Supplemental Resource Guide – Controls Management and CERT Resilience Management Model for additional guidance in establishing and maintaining controls management process.

See Appendix L – Controls Crosswalk for correlation of Cybersecurity Program controls with NIST 800-53 r4.

Appendix C – Change and Configuration Management Controls

Cyber Resilience Review Goals and Practices – Configuration and Change Management (CMM)

In order for a configuration and change management process to be considered valid and complete, at a minimum, the following objectives shall be addressed:

CMM.1 The lifecycle of assets is managed including:

- A change management process is used to manage modifications to assets.
- Resilience requirements are evaluated as a result of changes to assets.
- Capacity management and planning is performed for assets.
- Change requests are tracked to closure.
- Stakeholders are notified when they are affected by changes to assets.

CMM.2 The integrity of technology and information assets is managed including:

- Configuration management is performed for technology assets.
- Techniques are in use to detect changes to technology assets.
- Modifications to technology assets are reviewed.
- Integrity requirements are used to determine which staff members are authorized to modify information assets.
- The integrity of information assets is monitored.
- Unauthorized or unexplained modifications to technology assets are addressed.
- Modifications to technology assets are tested before being committed to production systems.
- A process for managing access to technology assets has been implemented.

CMM.3 Asset configuration baselines are established including:

- Technology assets have configuration baselines.
- Approval is obtained for proposed changes to configuration baselines.

Refer CRR Supplemental Resource Guide – Configuration & Change Management and CERT Resilience Management Model for additional guidance in establishing and maintaining configuration and change management process.

See Appendix L – Controls Crosswalk for correlation of Cybersecurity Program controls with NIST 800-53 r4.

Appendix D – Vulnerability Management Controls

Cyber Resilience Review Goals and Practices – Vulnerability Management (VM)

In order for a vulnerability management process to be considered valid and complete, at a minimum, the following objectives shall be addressed:

VM.1 Preparation for vulnerability analysis and resolution activities is conducted including:

- A vulnerability analysis and resolution strategy has been developed.
- There is a standard set of tools and/or methods in use to identify vulnerabilities in assets.

VM.2 A process for identifying and analyzing vulnerabilities is established and maintained including:

- Sources of vulnerability information have been identified.
- The information from these sources is kept current.
- Vulnerabilities are being actively discovered.
- Vulnerabilities are categorized and prioritized.
- Vulnerabilities are analyzed to determine relevance to the organization.
- A repository is used for recording information about vulnerabilities and their resolution.

VM.3 Exposure to identified vulnerabilities is managed including:

- Actions are taken to manage exposure to identified vulnerabilities.
- The effectiveness of vulnerability mitigation is reviewed.
- The status of unresolved vulnerabilities is monitored.

VM.4 The root causes of vulnerabilities are addressed including:

- Underlying causes for vulnerabilities are identified (through root-cause analysis or other means) and addressed.

Refer to CRR Supplemental Resource Guide – Vulnerability Management and CERT Resilience Management Model - Vulnerability Analysis and Resolution for additional guidance in establishing and maintaining a vulnerability management process.

See Appendix L – Controls Crosswalk for correlation of Cybersecurity Program controls with NIST 800-53 r4.

Appendix E – Incident Management Controls

Cyber Resilience Review Goals and Practices – Incident Management (IM)

In order for an incident management process to be considered valid and complete, at a minimum, the following objectives shall be addressed:

IM.1 A process for identifying, analyzing, responding to, and learning from incidents is established including:

- Each department has a plan for managing incidents.
- The incident management plan is reviewed and updated periodically.
- The roles and responsibilities in the plan are included in job descriptions.
- Staff have been assigned to the roles and responsibilities detailed in the incident management plan.

IM.2 A process for detecting, reporting, triaging, and analyzing events is established including:

- Events are detected and reported (to include cybersecurity events related to personnel activity, network activity, the physical environment, and information).
- Event data is logged in an incident knowledge base or similar mechanism.
- Events are categorized.
- Events are analyzed to determine if they are related to other events.
- Events are prioritized.
- The status of events is tracked.
- Events are managed to resolution.
- Requirements (rules, laws, regulations, policies, etc.) for identifying event evidence for forensic purposes have been identified.
- There is a process to ensure event evidence is handled as required by law or other obligations.

IM.3 Incidents are declared and analyzed including:

- Incidents are declared.
- Criteria for the declaration of an incident have been established.
- Incidents are analyzed to determine a response.

IM.4 A process for responding to and recovering from incidents is established including:

- Incidents are escalated to stakeholders for input and resolution.
- Responses to declared incidents are developed and implemented according to pre-defined procedures.
- Incident status and response are communicated to affected parties (including public relations staff and external media outlets).
- Incidents are tracked to resolution.

IM.5 Post-incident lessons learned are translated into improvement strategies including:

- Analysis is performed to determine the root causes of incidents.
- There is a link between the incident management process and other related processes (problem management, risk management, change management, etc.).

- Lessons learned from incident management is used to improve asset protection and service continuity strategies.

Refer to CRR Supplemental Resource Guide – Incident Management and CERT Resilience Management Model for additional guidance in establishing and maintaining an incident management process.

See Appendix L – Controls Crosswalk for correlation of Cybersecurity Program controls with NIST 800-53 r4.

Appendix F – Service Continuity Management Controls

Cyber Resilience Review Goals and Practices – Service Continuity Management (SC)

In order for a service continuity management process to be considered valid and complete, at a minimum, the following objectives shall be addressed:

SC.1 Service continuity plans for high-value services are developed including:

- Service continuity plans are developed and documented for assets required for delivery of the critical service.
- Service continuity plans are developed using established standards, guidelines, and templates.
- Staff members are assigned to execute specific service continuity plans.
- Key contacts are identified in the service continuity plans.
- Service continuity plans are stored in a controlled manner and available to all those who need to know.
- Availability requirements such as recovery time objectives and recovery point objectives are established.

SC.2 Service continuity plans are reviewed to resolve conflicts between plans including:

- Plans are reviewed to identify and resolve conflicts.

SC.3 Service continuity plans are tested to ensure they meet their stated objectives including:

- Standards for testing service continuity plans have been implemented.
- A schedule for testing service continuity plans has been established.
- Service continuity plans are tested.
- Backup and storage procedures for high-value information assets are tested.
- Test results are compared with test objectives to identify needed improvements to service continuity plans.

SC.4 Service continuity plans are executed and reviewed including:

- Conditions have been identified that trigger the execution of the service continuity plan.
- Execution of service continuity plans is reviewed.
- Improvements are identified as a result of executing service continuity plans.

Refer to CRR Supplemental Resource Guide – Service Continuity Management and CERT Resilience Management Model for additional guidance in establishing and maintaining a service continuity management process.

See Appendix L – Controls Crosswalk for correlation of Cybersecurity Program controls with NIST 800-53 r4.

Appendix G – Risk Management Controls

Cyber Resilience Review Goals and Practices – Risk Management (RM)

In order for a risk management process to be considered valid and complete, at a minimum, the following objectives shall be addressed:

RM.1 A strategy for identifying, analyzing, and mitigating risks is developed including:

- Sources of risk that can affect operations have been identified.
- Categories have been established for risks.
- A plan for managing operational risk has been established.
- The plan for managing operational risk is communicated to stakeholders.

RM.2 Risk tolerances are identified, and the focus of risk management activities is established including:

- Impact areas have been identified, such as reputation, financial health, and regulatory compliance.
- Impact areas have been prioritized to determine their relative importance.
- Risk tolerance parameters have been established for each impact area.
- Risk tolerance thresholds, which trigger action, are defined for each category of risk.

RM.3 Risks are identified including:

- Operational risks that could affect delivery of the critical service are identified.

RM.4 Risks are analyzed and assigned a disposition including:

- Risks are analyzed to determine potential impact to the critical service.
- A disposition (accept, transfer, mitigate, etc.) is assigned to identified risks.

RM.5 Risks to assets and services are mitigated and controlled including:

- Plans are developed for risks that the organization decides to mitigate.
- Identified risks are tracked to closure.

Refer to CRR Supplemental Resource Guide – Risk Management and CERT Resilience Management Model for additional guidance in establishing and maintaining an IT risk management process.

See Appendix L – Controls Crosswalk for correlation of Cybersecurity Program controls with NIST 800-53 r4.

Appendix H – External Dependencies Management Controls

Cyber Resilience Review Goals and Practices – External Dependencies Management (EDM)

In order for an external dependencies management process to be considered valid and complete, at a minimum, the following objectives shall be addressed:

EDM.1 External dependencies are identified and prioritized to ensure sustained operation of high-value services including:

- Dependencies on external relationships that are critical to the service are identified.
- A process has been established for creating and maintaining a list of external dependencies.
- External dependencies are prioritized.

EDM.2 Risks due to external dependencies are identified and managed.

EDM.3 Relationships with external entities are formally established and maintained including:

- Resilience requirements of the critical service have been established that apply specifically to each external dependency.
- These requirements are reviewed and updated.
- The ability of external entities to meet resilience requirements of the critical service is considered in the selection process.
- Resilience requirements are included in formal agreements with external entities.

EDM.4 Performance of external entities is managed including:

- The performance of external entities is monitored against resilience requirements.
- Responsibility has been assigned for monitoring external entity performance (as related to resilience requirements).
- Corrective actions are taken as necessary to address issues with external entities performance (as related to resilience requirements).
- Corrective actions are evaluated to ensure issues are remedied.

EDM.5 Dependencies on public services and infrastructure service providers are identified including:

- Public services on which the critical service depends (fire response and rescue services, law enforcement, etc.) are identified.
- Infrastructure providers on which the critical service depends (telecommunications and telephone services, energy sources, etc.) are identified.

Refer to CRR Supplemental Resource Guide – External Dependencies Management and CERT Resilience Management Model for additional guidance in establishing and maintaining an external dependencies management process.

See Appendix L – Controls Crosswalk for correlation of Cybersecurity Program controls with NIST 800-53 r4.

Appendix I – Training and Awareness Controls

Cyber Resilience Review Goals and Practices – Training and Awareness (TA)

In order for a training and awareness process to be considered valid and complete, at a minimum, the following objectives shall be addressed:

Note: **CRR Goal** and Practice [CERT-RMM reference]

TA.1 Cybersecurity awareness and training programs are established including:

- Cybersecurity awareness needs have been identified for the critical service.
- Required skills have been identified for specific roles (administrators, technicians, etc.) for the critical services.
- Skill gaps present in personnel responsible for cybersecurity are identified.
- Training needs have been identified.

TA.2 Awareness and training activities are conducted including:

- Cybersecurity awareness activities for the critical service are conducted.
- Cybersecurity training activities for the critical service are conducted.
- The effectiveness of the awareness and training programs is evaluated.
- Awareness and training activities are revised as needed.

Refer to CRR Supplemental Resource Guide – Training & Awareness and CERT Resilience Management Model for additional guidance in establishing and maintaining an IT security training and awareness process.

See Appendix L – Controls Crosswalk for correlation of Cybersecurity Program controls with NIST 800-53 r4.

Appendix J – Situational Awareness Controls

Cyber Resilience Review Goal and Practices – Situational Awareness (SA)

In order for a situational awareness process to be considered valid and complete, at a minimum, the following objectives shall be addressed:

SA.1 Threat monitoring is performed including:

- Responsibility for monitoring sources of threat information has been assigned.
- Threat monitoring procedures have been implemented.
- Resources have been assigned and trained to perform threat monitoring.

SA.2 The requirements for communicating threat information are established including:

- Internal stakeholders (such as critical service owner and incident management staff) have been identified to whom threat information must be communicated.
- External stakeholders (such as emergency management personnel, regulatory, and information sharing organizations) have been identified to whom threat information must be communicated.

SA.3 Threat information is communicated including:

- Threat information is communicated to stakeholders.
- Resources have been assigned authority and accountability for communicating threat information.
- Resources have been trained with respect to their specific role in communicating threat information.

Refer to CRR Supplemental Resource Guide – Situational Awareness and CERT Resilience Management Model for additional guidance in establishing and maintaining an IT situational awareness program.

See Appendix L – Controls Crosswalk for correlation of Cybersecurity Program controls with NIST 800-53 r4.

Appendix K – Listing of State and Federal Laws and Regulations

The following is a selected list (from State of California Office of the Attorney General) of security and privacy laws and regulations that may be applicable to County departments. It is not meant to be a comprehensive listing of all applicable security and privacy laws and regulations.

Health Insurance Portability and Accountability Act of 1996 (HIPAA). 45 CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information and Security Standards for the Protection of Electronic Protected Health Information. HIPAA includes provisions designed to save money for health care businesses by encouraging electronic transactions and also regulations to protect the security and confidentiality of patient information. The privacy rule took effect on April 14, 2001, with most covered entities (health plans, health care clearinghouse and health care providers who conduct certain financial and administrative transactions electronically) having until April 2003 to comply. The security rule took effect on April 21, 2003.

Court Records: Protection of Victim and Witness Information - California Penal Code section 964. This law requires the district attorney and the courts in each county to establish a procedure to protect confidential personal information regarding any witness or victim contained in a police report, arrest report, or investigative report submitted to a court by a prosecutor in support of a criminal complaint, indictment, or information, or by a prosecutor or law enforcement officer in support of a search warrant or an arrest warrant.

Credit Card or Check Payment - California Civil Code sections 1725 and 1747.08. Any person accepting a check in payment for most goods or services at retail is prohibited from recording a purchaser's credit card number or requiring that a credit card be shown as a condition of accepting the check (Section 1725). Any person accepting a credit card in payment for most goods or services is prohibited from writing the collecting and recording cardholder's personal information on forms associated with the transaction. The law explicitly allows the collection of a zip code in a sales transaction at a gas pump or an automated cashier in a gas station and limits the use of the zip code information to the prevention of fraud. (Section 1747.08).

Credit/Debit Card Number Truncation - California Civil Code section 1747.09. No more than the last five digits of a credit card or debit card number may be printed on the customer copy of electronically printed receipts.

Data Breach Notice - California Civil Code sections 1798.29 and 1798.82. This law requires a business or a government agency that owns or licenses unencrypted computerized data that includes personal information, as defined, to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The type of information that triggers the notice requirement is 1) an individual's name plus one or more of the following: Social Security number, driver's license or California Identification Card number, financial account numbers, medical information, health insurance, or information collected through an automated license plate recognition system; or 2) user ID and password or other specified credentials permitting access to online accounts. The notice must contain specific information, and it must use a title and headings, as specified. Any agency, person, or business that is required to issue a breach notice to more than 500 California residents must electronically submit a single sample copy to the Attorney General.

Disposal of Customer Records - California Civil Code sections 1798.80 - 1798.81 and 1798.84. These sections require businesses to shred, erase or otherwise modify the personal information when disposing of customer records under their control. It provides a "safe harbor" from civil litigation for a business that has come into possession of records containing personal information that were abandoned, so long as the business disposes of them as provided in the statute.

Library Records, Confidentiality - California Government Code sections 6254, 6267 and 6276.28. Registration and circulation records, of libraries supported by public funds, are confidential and are explicitly exempted from the Public Records Act.

Marriage Records - California Family Code section 509, California Health and Safety Code sections 102230, 102231, 103525, 103525.5, 103526, 103526.5 and 103527. These laws establish procedures for requesting a certified copy of a birth or death records. They also provide protection of specified confidential information in these records, including in marriage records. The law also requires that non-confidential marriage files contain the names of the parties and the date of the marriage.

Public Records Act - California Government Code sections 6250-6268. This law applies to state and local government. It gives members of the public a right to obtain certain described kinds of documents that are not protected from disclosure by the Constitution and other laws. This law also provides some specific privacy protections.

Security of Personal Information - California Civil Code section 1798.81.5. This law requires specified businesses to use safeguards to ensure the security of Californians' personal information (defined as name plus Social Security Number (SSN), driver's license or state ID, financial account number, username or email address in combination with password or security question and answer, and health insurance information) and to contractually require third parties to do the same. It does not apply to businesses that are subject to certain other information security laws.

Social Security Number Confidentiality - California Civil Code sections 1798.85 and 1798.86, 1785.11.1, and 1785.11.6. This law restricts businesses and state and local agencies from publicly posting or displaying Social Security numbers. It also bans embedding SSNs on a card or document using a bar code, chip, magnetic strip or other technology, in place of removing the number as required by law. The law takes effect gradually, from 2002 through 2007. See the Recommended Practices in relation to this law.

Social Security Numbers in Local Government Records and Higher Education - California Civil Code section 1798.89, Commercial Code section 9526.5, Education Code section 66018.55, and Government Code section 27300 et seq. These laws require certain state and local government agencies to truncate SSNs in documents released to the public so as to display no more than the last four digits. (1) The Franchise Tax Board must truncate SSNs in documents released to the public. (2) The Secretary of State must create versions of Uniform Commercial Code filings that contain only truncated SSNs. (3) County recorders must create versions of documents recorded back to 1980 that contain only truncated SSNs, and if authorized by boards of supervisors may levy a fee to cover the cost of truncation. Also no one may record a document containing more than the last four digits of an SSN. (4) The law states the Legislature's intent that local agencies, other than county recorders, fully redact SSNs from public records before making the records publicly available, and excludes SSNs from the information that a local agency must disclose under the Public Records Act. (5) It requires the Office of Privacy Protection to create a task force to review the use of SSNs by California colleges and universities and to recommend practices to minimize such use, with a report due to the Legislature by July 1, 2010.

State Agencies: Information Security - Government Code § 11549.3. This law requires the California Information Security Office, in the Department of Technology, to conduct or require at least 35 independent security assessments of state agencies annually.

Voter Privacy - California Elections Code sections 2194, 8105, 8202, 8204, 2166.7 and 8023, and California Government Code 6254.24. If authorized by a local board of supervisors, a local election official must make the voter registration information of specified public safety officials confidential, upon application. The application of a public safety official for confidentiality would be a public record. The law also includes a voter's signature on a voter registration card as part of confidential voter registration information and adds state and federal judges and court commissioners to the definition of public safety officials entitled to remove their home addresses and telephone numbers from public posting on the Internet.

The following are additional selected security and privacy regulations that may be applicable to County departments:

The **Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act)** is a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies. The FTC has brought many enforcement actions against companies failing to comply with posted privacy policies and for the unauthorized disclosure of personal data. The FTC is also the primary enforcer of the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§6501-6506), which applies to the online collection of information from children, and the Self-Regulatory Principles for Behavioral Advertising.

The **Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827)** regulates the collection, use and disclosure of financial information. It can apply broadly to financial institutions such as banks, securities firms and insurance companies, and to other businesses that provide financial services and products. GLB limits the disclosure of non-public personal information, and in some cases requires financial institutions to provide notice of their privacy practices and an opportunity for data subjects to opt out of having their information shared. In addition, there are several Privacy Rules promulgated by national banking agencies and the Safeguards Rule, Disposal Rule, and Red Flags Rule issued by the FTC that relate to the protection and disposal of financial data. The GLB Act regulates the collection, use, sharing and disclosure of non-public financial information. The requirements for written notice of privacy procedures and obtaining consent (and opportunities to opt-out of certain disclosures) vary depending on whether the data subject is a customer or a consumer and with whom the financial institution shares this information. One of the most onerous obligations financial institutions is to implement a security program to protect the non-public personal information from unauthorized disclosures.

Health Information Technology for Economic and Clinical Health (HITECH) Act (the Final Omnibus Rule)

Title 42, USC § 290dd–2

Title 42, CFR Part2

Title 42, CFR Part 96, § 96.132(e)

Title 42, USC §§ 1320d through 1320d-8

Welfare and Institutional code, § 14100.2, which is specific to Medi-Cal

HSC §§ 11812 and 11845.5

HSC §§ 123110 through 123149.5 – Patient Access to Health Records

Title 22, CCR § 51009, which is specific to Medi-Cal

Civil Code §§ 56 through 56.37 – Confidentiality of Medical Information Act

Civil Code §§ 1798.80 through 1798.82 – Customer Records (breach of security)

Civil Code § 1798.85 – Confidentiality of Social Security Number

The American Recovery and Reinvestment Act of 2009 (ARRA) Electronic Health Records (EHR) Incentive Program – Meaningful Use

The following are additional selected security and privacy requirements that may be applicable to County departments:

U.S. Department of Justice Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy. The CJIS Security Policy provides Criminal Justice Agencies and Noncriminal Justice Agencies with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

State of California Department of Motor Vehicles Information Security Agreement. Agreement must be completed by organizations requesting a connection to DMV. The DMV ISA uses information security standards and guidelines derived from NIST SP 800-53, to reinforce the information security requirements of the DMV for electronic access or connection. Together, the NIST and DMV security requirements provide a robust baseline of security controls. These controls are essential for protecting the confidentiality, integrity, and availability of DMV information and the information systems authorized to process, store, and transmit that information.

Medi-Cal Privacy and Security Agreement. The Department of Health Care Services (DHCS) and the County of Orange, Social Services Agency enter into this Medi-Cal Data Privacy and Security Agreement (Agreement) in order to ensure the privacy and security of Medi-Cal Personally Identifiable Information (PII).

Payment Card Industry-Data Security Standard (PCI-DSS). PCI Security Standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with requirements for software developers and manufacturers of applications and devices used in those transactions. The Council is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB, MasterCard and Visa Inc.

Appendix L – Controls Crosswalk

Subject	CRR Number	CRR Control Description	NIST 800.53
Asset Management			
		1. Services are identified and prioritized	
	AM.1.1	Are services identified?	
	AM.1.2	Are services prioritized based on analysis of the potential impact if the services are disrupted?	CP-2 RA-2 SA-14
	AM.1.3	Is the organization's mission, vision, values and purpose, including the organization's place in critical infrastructure, identified, and communicated?	PM-8
	AM.1.4	Are the organization's mission, objectives, and activities prioritized?	SA-14 PM-11
		2. Assets are inventoried, and the authority and responsibility for these assets is established.	
	AM.2.1	Are the assets that directly support the critical service inventoried (technology includes hardware, software, and external information systems)?	
		People	
		Information	
		Technology	AC-20 CM-8 SA-9
		Facilities	
	AM.2.2	Do asset descriptions include protection and sustainment requirements?	
		People	
		Information	
		Technology	
		Facilities	
	AM.2.3	Are both owners and custodians of assets documented in asset descriptions?	
		People	
		Information	
		Technology	
		Facilities	
	AM.2.4	Are the physical locations of assets (both within and outside the organization) documented in the asset inventory?	
		People	
		Information	
		Technology	
		Facilities	
	AM.2.5	Are organizational communications and data flows mapped and documented in the asset inventory?	AC-4 CA-3 CA-9 PL-8
		3. The relationship between assets and the services they support is established.	

Subject	CRR Number	CRR Control Description	NIST 800.53
	AM.3.1	Are the associations between assets and the critical service they support documented?	CP-8 PE-9 PE-11 SA-14 PM-8
		People	CP-8 PE-9 PE-11 SA-14 PM-8
		Information	CP-8 PE-9 PE-11 SA-14 PM-8
		Technology	CP-8 PE-9 PE-11 SA-14 PM-8
		Facilities	CP-8 PE-9 PE-11 SA-14 PM-8
	AM.3.2	Are confidentiality, integrity, and availability requirements established for each service-related asset?	
		People	
		Information	
		Technology	
		Facilities	
		4. The asset inventory is managed.	
	AM.4.1	Have change criteria been established for asset descriptions?	
		People	
		Information	
		Technology	
		Facilities	
	AM.4.2	Are asset descriptions updated when changes to assets occur?	
		People	
		Information	
		Technology	
		Facilities	
		5. Access to assets is managed.	
	AM.5.1	Is access (including identities and credentials) to assets granted based on their protection requirements?	AC-2 AC-17 AC-18 AC-20 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-7 IA-8 IA-9 IA-10 IA-11 PE-2 PE-3 PE-4 PE-5 PE-6 PE-9
		Information	AC-2 AC-17 AC-18 AC-20 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-7 IA-8 IA-9 IA-10 IA-11 PE-2 PE-3 PE-4 PE-5 PE-6 PE-9
		Technology	AC-2 AC-17 AC-18 AC-20 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-

Subject	CRR Number	CRR Control Description	NIST 800.53
			7 IA-8 IA-9 IA-10 IA-11 PE-2 PE-3 PE-4 PE-5 PE-6 PE-9
		Facilities	AC-2 AC-17 AC-18 AC-20 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-7 IA-8 IA-9 IA-10 IA-11 PE-2 PE-3 PE-4 PE-5 PE-6 PE-9
	AM.5.2	Are access (including identities and credentials) requests reviewed and approved by the asset owner?	AC-2 AC-17 AC-18 AC-20 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-7 IA-8 IA-9 IA-10 IA-11 PE-2 PE-3 PE-4 PE-5 PE-6 PE-9
		Information	AC-2 AC-17 AC-18 AC-20 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-7 IA-8 IA-9 IA-10 IA-11 PE-2 PE-3 PE-4 PE-5 PE-6 PE-9
		Technology	AC-2 AC-17 AC-18 AC-20 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-7 IA-8 IA-9 IA-10 IA-11 PE-2 PE-3 PE-4 PE-5 PE-6 PE-9
		Facilities	AC-2 AC-17 AC-18 AC-20 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-7 IA-8 IA-9 IA-10 IA-11 PE-2 PE-3 PE-4 PE-5 PE-6 PE-9
	AM.5.3	Are access privileges reviewed to identify excessive or inappropriate privileges?	
		Information	
		Technology	
		Facilities	
	AM.5.4	Are access privileges modified as a result of reviews?	
		Information	
		Technology	
		Facilities	

Subject	CRR Number	CRR Control Description	NIST 800.53
	AM.5.5	Are access permissions managed incorporating the principle of least privilege?	AC-2 AC-3 AC-5 AC-6 AC-16
		Information	AC-2 AC-3 AC-5 AC-6 AC-16
		Technology	AC-2 AC-3 AC-5 AC-6 AC-16
		Facilities	AC-2 AC-3 AC-5 AC-6 AC-16
	AM.5.6	Are access permissions managed incorporating the principle of separation of duties?	AC-2 AC-3 AC-5 AC-6 AC-16
		Information	AC-2 AC-3 AC-5 AC-6 AC-16
		Technology	AC-2 AC-3 AC-5 AC-6 AC-16
		Facilities	AC-2 AC-3 AC-5 AC-6 AC-16
		6. Information assets are categorized and managed to ensure the sustainment and protection of the critical service.	
	AM.6.1	Are information assets categorized based on sensitivity and potential impact to the critical service (such as public, internal use only, secret)?	
	AM.6.2	Is the categorization of information assets monitored and enforced?	
	AM.6.3	Are there policies and procedures for the proper labeling and handling of information assets?	
	AM.6.4	Are all staff members who handle information assets (including those who are external to the organization, such as contractors) trained in the use of information categories?	AT-2 PM-13
	AM.6.5	Are high-value information assets backed-up and retained?	CP-4 CP-6 CP-9
	AM.6.6	Do guidelines exist for properly disposing of information assets?	CM-8 MP-6 PE-16
	AM.6.7	Is adherence to information asset disposal guidelines monitored and enforced?	CM-8 MP-6 PE-16
		7. Facility assets supporting the critical service are prioritized and managed.	
	AM.7.1	Are facilities prioritized based on potential impact to the critical service, to identify those that should be the focus of protection and sustainment activities?	CP-2 CP-8 PE-9 PE-11 RA-2 SA-14 PM-8
	AM.7.2	Is the prioritization of facilities reviewed and validated?	CP-2 CP-8 PE-9 PE-11 RA-2 SA-14 PM-8
	AM.7.3	Are protection and sustainment requirements of the critical service considered during the selection of facilities?	PE-10 PE-12 PE-13 PE-14 PE-15 PE-18

Subject	CRR Number	CRR Control Description	NIST 800.53
		Maturity Indicator Level	
	AM.MIL2.1	Is there a documented plan for performing asset management activities?	
	AM.MIL2.2	Is there a documented policy for asset management?	
	AM.MIL2.3	Have stakeholders for asset management activities been identified and made aware of their roles?	CP-2 PS-7 PM-1 PM-11
	AM.MIL2.4	Have asset management standards and guidelines been identified and implemented?	
	AM.MIL3.1	Is there management oversight of the performance of the asset management activities?	AC-21 CA-7 SI-4
	AM.MIL3.2	Have qualified staff been assigned to perform asset management activities as planned?	
	AM.MIL3.3	Is there adequate funding to perform asset management activities as planned?	
	AM.MIL3.4	Are risks related to the performance of planned asset management activities identified, analyzed, disposed of, monitored, and controlled?	PM-4 PM-9 PM-11
	AM.MIL4.1	Are asset management activities periodically reviewed and measured to ensure they are effective and producing intended results?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	AM.MIL4.2	Are asset management activities periodically reviewed to ensure they are adhering to the plan?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	AM.MIL4.3	Is higher-level management aware of issues related to the performance of asset management?	AC-21 CA-7 SI-4
	AM.MIL5.1	Has the organization adopted a standard definition of asset management activities from which operating units can derive practices that fit their unique operating circumstances?	
	AM.MIL5.2	Are improvements to asset management activities documented and shared across the organization?	
Controls Management			
		1. Control objectives are established	
	CM.1.1	Have control objectives been established for assets required for delivery of the critical service?	
		People	
		Information	
		Technology	
		Facilities	
	CM.1.2	Are control objectives prioritized according to their potential to affect the critical service?	
		2. Controls are implemented	
	CM.2.1	Have controls been implemented to achieve the control objectives established for the critical service?	

Subject	CRR Number	CRR Control Description	NIST 800.53
	CM.2.2	Have controls been implemented, incorporating network segregation where appropriate, to protect network integrity?	AC-4 SC-7 SC-28
	CM.2.3	Have controls been implemented to protect data-at-rest?	
	CM.2.4	Have controls been implemented to protect data-in-transit?	SC-8
	CM.2.5	Have controls been implemented to protect against data leaks?	AC-4 AC-5 AC-6 PE-19 PS-3 PS-6 SC-7 SC-8 SC-13 SC-31 SI-4
	CM.2.6	Have audit/log records been determined, documented, implemented, and reviewed in accordance with policy?	AU-1 AU-2 AU-3 AU-4 AU-5 AU-6 AU-7 AU-8 AU-9 AU-10 AU-11 AU-12 AU-13 AU-14 AU-15 AU-16
	CM.2.7	Have controls been implemented to protect and restrict the use of removable media in accordance with policy?	MP-2 MP-4 MP-5 MP-7
	CM.2.8	Have controls been implemented to protect communication and control networks?	AC-4 AC-17 AC-18 CP-8 SC-7
	CM.2.9	Have cybersecurity human resource practices been implemented for the critical service (e.g., de-provisioning, personnel screening)?	PS-1 PS-2 PS-3 PS-4 PS-5 PS-6 PS-7 PS-8
	CM.2.10	Is access to systems and assets controlled by incorporating the principle of least functionality (e.g., whitelisting, blacklisting, etc.)?	AC-3
		3. Control designs are analyzed to ensure they satisfy control objectives.	
	CM.3.1	Are control designs analyzed to identify gaps where control objectives are not adequately satisfied?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
		People	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
		Information	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
		Technology	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
		Facilities	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	CM.3.2	As a result of the controls analysis, are new controls introduced or existing controls modified to address gaps?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
		4. The internal control system is assessed to ensure control objectives are met.	
	CM.4.1	Is the performance of controls assessed on a scheduled basis to verify they continue to meet control objectives?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6

Subject	CRR Number	CRR Control Description	NIST 800.53
		People	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
		Information	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
		Technology	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
		Facilities	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	CM.4.2	As a result of scheduled assessments, are new controls introduced or existing controls modified to address problem areas?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
		Maturity Indicator Level	
	CM.MIL2.1	Is there a plan for performing controls management activities?	
	CM.MIL2.2	Is there a documented policy for controls management?	
	CM.MIL2.3	Have stakeholders for controls management activities have been identified and made aware of their roles?	CP-2 PS-7 PM-1 PM-11
	CM.MIL2.4	Have controls management standards and guidelines been identified and implemented?	
	CM.MIL3.1	Is there management oversight of the performance of the controls management activities?	AC-21 CA-7 SI-4
	CM.MIL3.2	Have qualified staff been assigned to perform controls management activities as planned?	
	CM.MIL3.3	Is there adequate funding to perform controls management activities as planned?	
	CM.MIL3.4	Are risks related to the performance of planned controls management activities identified, analyzed, disposed of, monitored, and controlled?	PM-4 PM-9 PM-11
	CM.MIL4.1	Are controls management activities periodically reviewed and measured to ensure they are effective and producing intended results?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	CM.MIL4.2	Are controls management activities periodically reviewed to ensure they are adhering to the plan?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	CM.MIL4.3	Is higher-level management aware of issues related to the performance of controls management?	AC-21 CA-7 SI-4
	CM.MIL5.1	Has the organization adopted a standard definition of controls management activities from which operating units can derive practices that fit their unique operating circumstances?	
	CM.MIL5.2	Are improvements to controls management documented and shared across the organization?	
Configuration and Change Management			
		1. The life cycle of assets is managed.	
	CCM.1.1	Is a change management process used to manage modifications to assets?	CM-3 CM-4 SA-10

Subject	CRR Number	CRR Control Description	NIST 800.53
		Information	CM-3 SA-10
		Technology	CM-3 SA-10
		Facilities	CM-3 SA-10
	CCM.1.2	Are resilience requirements evaluated as a result of changes to assets?	CM-3 CM-4 SA-10
		Information	CM-3 SA-10
		Technology	CM-3 SA-10
		Facilities	CM-3 SA-10
	CCM.1.3	Is capacity management and planning performed for assets?	CP-2 SC-5
	CCM.1.4	Are change requests tracked to closure?	CM-3 CM-4 SA-10
	CCM.1.5	Are stakeholders notified when they are affected by changes to assets?	CM-3 CM-4 SA-10
	CCM.1.6	Is a System Development Life Cycle implemented to manage systems supporting the critical service?	PL-8 SA-3 SA-4 SA-8 SA-10 SA-11 SA-12 SA-15 SA-17
		2. The integrity of technology and information assets is managed	
	CCM.2.1	Is configuration management performed for technology assets?	CM-2 CM-3 CM-4 CM-5 CM-6 CM-7 CM-9 SA-10
	CCM.2.2	Are techniques in use to detect changes to technology assets?	SI-7
	CCM.2.3	Are modifications to technology assets reviewed?	CM-2 CM-3 CM-4 CM-5 CM-6 CM-7 CM-9 SA-10
	CCM.2.4	Are integrity requirements used to determine which staff members are authorized to modify information assets?	AC-2 AC-3 AC-5 AC-6 AC-16 CM-3 CM-4 PS-1 PS-2 PS-3 PS-4 PS-5 PS-6 PS-7 PS-8 SA-10
	CCM.2.5	Is the integrity of information assets monitored?	SI-7
	CCM.2.6	Are unauthorized or unexplained modifications to technology assets addressed?	CM-3 CM-4 SA-10
	CCM.2.7	Are modifications to technology assets tested before being committed to production systems?	CM-2
	CCM.2.8	Has a process for managing access to technology assets been implemented?	
	CCM.2.9	Is the maintenance and repair of assets performed and logged in a timely manner?	MA-2 MA-3 MA-5
	CCM.2.10	Is the maintenance and repair of assets performed with approved and controlled tools and/or methods?	CM-7 MA-2 MA-3 MA-5
	CCM.2.11	Is the remote maintenance and repair of assets approved, logged, and performed in a manner that prevents unauthorized access?	MA-4

Subject	CRR Number	CRR Control Description	NIST 800.53
		3. Asset configuration baselines are established	
	CCM.3.1	Do technology assets have configuration baselines?	CM-2 CM-3 CM-4 CM-5 CM-6 CM-7 CM-9 SA-10
	CCM.3.2	Is approval obtained for proposed changes to baselines?	CM-2 CM-3 CM-4 CM-5 CM-6 CM-7 CM-9 SA-10
	CCM.3.3	Has a baseline of network operations been established?	AC-4 CA-3 CM-2 SI-4
	CCM.3.4	Is the baseline of network operations managed?	AC-4 CA-3 CM-2 SI-4
	CCM.3.5	Has a baseline of expected data flows for users and systems been established?	AC-4 CA-3 CM-2 SI-4
	CCM.3.6	Is the baseline of expected data flows for users and systems managed?	AC-4 CA-3 CM-2 SI-4
		Maturity Indicator Level	
	CCM.MIL2.1	Is there a documented plan for performing change management activities?	
	CCM.MIL2.2	Is there a documented policy for change management?	
	CCM.MIL2.3	Have stakeholders for change management activities been identified and made aware of their roles?	CP-2 PS-7 PM-1 PM-11
	CCM.MIL2.4	Have change management standards and guidelines been identified and implemented?	
	CCM.MIL3.1	Is there management oversight of the performance of the change management activities?	AC-21 CA-7 SI-4
	CCM.MIL3.2	Have qualified staff been assigned to perform change management activities as planned?	
	CCM.MIL3.3	Is there adequate funding to perform change management activities as planned?	
	CCM.MIL3.4	Are risks related to the performance of planned change management activities identified, analyzed, disposed of, monitored, and controlled?	PM-4 PM-9 PM-11
	CCM.MIL4.1	Are change management activities periodically reviewed and measured to ensure they are effective and producing intended results?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	CCM.MIL4.2	Are change management activities periodically reviewed to ensure they are adhering to the plan?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	CCM.MIL4.3	Is higher-level management aware of issues related to the performance of change management?	AC-21 CA-7 SI-4
	CCM.MIL5.1	Has the organization adopted a standard definition of change management activities from which operating units can derive practices that fit their unique operating circumstances?	

Subject	CRR Number	CRR Control Description	NIST 800.53
	CCM.MIL5.2	Are improvements to change management documented and shared across the organization?	
Vulnerability Management			
		1. Preparation for vulnerability analysis and resolution activities is conducted.	
	VM.1.1	Has a vulnerability analysis and resolution strategy been developed?	RA-3 RA-5 SI-2
		People	RA-3 RA-5 SI-2
		Information	RA-3 RA-5 SI-2
		Technology	RA-3 RA-5 SI-2
		Facilities	RA-3 RA-5 SI-2
	VM.1.2	Is there a standard set of tools and/or methods in use to identify vulnerabilities in assets?	
		People	
		Information	
		Technology	
		Facilities	
	VM.1.3	Is there a standard set of tools and/or methods in use to detect malicious code in assets?	SI-3
	VM.1.4	Is there a standard set of tools and/or methods in use to detect unauthorized mobile code in assets?	SC-18 SC-44 SI-4
	VM.1.5	Is there a standard set of tools and/or methods in use to monitor assets for unauthorized personnel, connections, devices, and software?	AU-12 CA-7 CM-3 CM-8 PE-3 PE-6 PE-20 SI-4
		2. A process for identifying and analyzing vulnerabilities is established and maintained.	
	VM.2.1	Have sources of vulnerability information been identified?	SI-5 PM-15 PM-16
		Information	SI-5 PM-15 PM-16
		Technology	SI-5 PM-15 PM-16
		Facilities	SI-5 PM-15 PM-16
	VM.2.2	Is the information from these sources kept current?	CA-2 CA-7 CP-2 IR-8 PL-2 RA-5 SI-4 SI-5 PM-6 PM-14 PM-15 PM-16
		Information	CA-2 CA-7 CP-2 IR-8 PL-2 RA-5 SI-4 SI-5 PM-6 PM-14 PM-15 PM-16
		Technology	CA-2 CA-7 CP-2 IR-8 PL-2 RA-5 SI-4 SI-5 PM-6 PM-14 PM-15 PM-16

Subject	CRR Number	CRR Control Description	NIST 800.53
		Facilities	CA-2 CA-7 CP-2 IR-8 PL-2 RA-5 SI-4 SI-5 PM-6 PM-14 PM-15 PM-16
	VM.2.3	Are vulnerabilities being actively discovered?	CA-2 CA-7 CA-8 RA-3 RA-5 SA-5 SA-11 SI-2 SI-4 SI-5
		Information	CA-2 CA-7 CA-8 RA-3 RA-5 SA-5 SA-11 SI-2 SI-4 SI-5
		Technology	CA-2 CA-7 CA-8 RA-3 RA-5 SA-5 SA-11 SI-2 SI-4 SI-5
		Facilities	CA-2 CA-7 CA-8 RA-3 RA-5 SA-5 SA-11 SI-2 SI-4 SI-5
	VM.2.4	Are vulnerabilities categorized and prioritized?	RA-3 RA-5 SI-2
		Information	RA-3 RA-5 SI-2
		Technology	RA-3 RA-5 SI-2
		Facilities	RA-3 RA-5 SI-2
	VM.2.5	Are vulnerabilities analyzed to determine relevance to the organization?	RA-3 RA-5 SI-2
		Information	RA-3 RA-5 SI-2
		Technology	RA-3 RA-5 SI-2
		Facilities	RA-3 RA-5 SI-2
	VM.2.6	Is a repository used for recording information about vulnerabilities and their resolution?	CA-2 CA-7 CA-8 RA-3 RA-5 SA-5 SA-11 SI-2 SI-4 SI-5
		Information	CA-2 CA-7 CA-8 RA-3 RA-5 SA-5 SA-11 SI-2 SI-4 SI-5
		Technology	CA-2 CA-7 CA-8 RA-3 RA-5 SA-5 SA-11 SI-2 SI-4 SI-5
		Facilities	CA-2 CA-7 CA-8 RA-3 RA-5 SA-5 SA-11 SI-2 SI-4 SI-5
		3. Exposure to identified vulnerabilities is managed	
	VM.3.1	Are actions taken to manage exposure to identified vulnerabilities?	CA-7 RA-3 RA-5
	VM.3.2	Is the effectiveness of vulnerability mitigation reviewed?	CA-2 CA-7 CP-2 IR-8 PL-2 RA-5 SI-4 PM-6 PM-14

Subject	CRR Number	CRR Control Description	NIST 800.53
	VM.3.3	Is the status of unresolved vulnerabilities monitored?	RA-3 RA-5 SI-2
		4. The root causes of vulnerabilities are addressed	
	VM.4.1	Are underlying causes for vulnerabilities identified (through root-cause analysis or other means) and addressed?	RA-3 RA-5 SI-2
		Maturity Indicator Level	
	VM.MIL2.1	Is there a documented plan for performing vulnerability management activities?	RA-3 RA-5 SI-2
	VM.MIL2.2	Is there a documented policy for vulnerability management?	
	VM.MIL2.3	Have stakeholders for vulnerability management activities been identified and made aware of their roles?	CP-2 PS-7 PM-1 PM-11
	VM.MIL2.4	Have vulnerability management standards and guidelines been identified and implemented?	RA-3 RA-5 SI-2
	VM.MIL3.1	Is there management oversight of the performance of the vulnerability management activities?	AC-21 CA-7 SI-4
	VM.MIL3.2	Have qualified staff been assigned to perform vulnerability management activities as planned?	
	VM.MIL3.3	Is there adequate funding to perform vulnerability management activities as planned?	
	VM.MIL3.4	Are risks related to the performance of planned vulnerability management activities identified, analyzed, disposed of, monitored, and controlled?	PM-4 PM-9 PM-11
	VM.MIL4.1	Are vulnerability management activities periodically reviewed and measured to ensure they are effective and producing intended results?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	VM.MIL4.2	Are vulnerability management activities periodically reviewed to ensure they are adhering to the plan?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	VM.MIL4.3	Is higher-level management aware of issues related to the performance of vulnerability management?	AC-21 CA-7 SI-4
	VM.MIL5.1	Has the organization adopted a standard definition of vulnerability management activities from which operating units can derive practices that fit their unique operating circumstances?	
	VM.MIL5.2	Are improvements to vulnerability management activities documented and shared across the organization?	
Incident Management			
		1. A process for identifying, analyzing, responding to, and learning from incidents is established	
	IM.1.1	Does the organization have a plan for managing incidents?	CA-2 CA-7 CP-2 IR-8 PM-14
	IM.1.2	Is the incident management plan reviewed and updated?	CA-2 CA-7 CP-4 IR-3 PL-2 RA-5 SI-4 PM-14

Subject	CRR Number	CRR Control Description	NIST 800.53
	IM.1.3	Are the roles and responsibilities in the plan included in job descriptions?	CA-2 CA-7 PS-1 PS-2 PS-3 PS-4 PS-5 PS-6 PS-7 PS-8 PM-14
	IM.1.4	Have staff been assigned to the roles and responsibilities detailed in the incident management plan?	CA-2 CA-7 CP-2 CP-3 IR-3 IR-8 PM-14
		2. A process for detecting, reporting, triaging, and analyzing events is established	
	IM.2.1	Are events detected and reported (to include cybersecurity events related to personnel activity, network activity, the physical environment, and information)?	AC-2 AU-6 AU-12 AU-13 CA-2 CA-7 CM-3 CM-10 CM-11 IR-6 IR-8 PE-3 PE-6 PE-20 RA-5 SC-5 SC-7 SI-4
	IM.2.2	Is event data logged in an incident knowledgebase or similar mechanism?	AU-6 CA-7 IR-4 IR-5 IR-8 SI-4
	IM.2.3	Are events categorized?	CP-2 IR-4 IR-5 IR-8
	IM.2.4	Are events analyzed to determine if they are related to other events?	AU-6 CA-7 IR-4 IR-5 IR-8 SI-4
	IM.2.5	Are events prioritized?	CP-2 IR-4 PS-3 SI-4
	IM.2.6	Is the status of events tracked?	AU-6 CA-7 IR-4 IR-5 IR-8 SI-4
	IM.2.7	Are events managed to resolution?	AU-6 CA-7 IR-4 IR-5 IR-8 PE-6 SI-4
	IM.2.8	Have requirements (rules, laws, regulations, policies, etc.) for identifying event evidence for forensic purposes been identified?	CA-2 CA-7 SI-4 PM-14
	IM.2.9	Is there a process to ensure event evidence is handled as required by law or other obligations?	AU-7 IR-4
		3. Incidents are declared and analyzed.	
	IM.3.1	Are incidents declared?	AU-6 IR-6 IR-8
	IM.3.2	Have criteria for the declaration of an incident been established?	IR-4 IR-5 IR-8
	IM.3.3	Are incidents analyzed to determine a response?	CP-2 IR-4 IR-5 IR-8
		4. A process for responding to and recovering from incidents is established.	
	IM.4.1	Are incidents escalated to stakeholders for input and resolution?	CP-2 IR-4 IR-8
	IM.4.2	Are responses to declared incidents developed and implemented according to pre-defined procedures?	CP-2 CP-10 IR-4 IR-8
	IM.4.3	Are incident status and response communicated to affected parties (including public relations staff and external media outlets)?	CA-2 CA-7 CP-2 IR-4 IR-8 PE-6 RA-5 SI-4

Subject	CRR Number	CRR Control Description	NIST 800.53
	IM.4.4	Are incidents tracked to resolution?	IR-4
		5. Post-incident lessons learned are translated into improvement strategies.	
	IM.5.1	Is analysis performed to determine the root causes of incidents?	CA-2 CA-7 CP-2 IR-8 PL-2 RA-5 SI-4 PM-6 PM-14
	IM.5.2	Is there a link between the incident management process and other related processes (problem management, risk management, change management, etc.)?	CA-2 CA-7 CP-2 IR-8 PL-2 RA-5 SI-4 PM-6 PM-14
	IM.5.3	Are lessons learned from incident management used to improve asset protection and service continuity strategies?	CA-2 CA-7 CP-2 IR-4 IR-8 PL-2 RA-5 SI-4 PM-6 PM-14
		Maturity Indicator Level	
	IM.MIL2.1	Is there a documented plan for performing incident management activities?	CP-2 IR-8
	IM.MIL2.2	Is there a documented policy for incident management?	
	IM.MIL2.3	Have stakeholders for incident management activities been identified and made aware of their roles?	CP-2 PS-7 PM-1 PM-11
	IM.MIL2.4	Have incident management standards and guidelines been identified and implemented?	CP-2 IR-8
	IM.MIL3.1	Is there management oversight of the performance of the incident management activities?	AC-21 CA-7 SI-4
	IM.MIL3.2	Have qualified staff been assigned to perform incident management activities as planned?	
	IM.MIL3.3	Is there adequate funding to perform incident management activities as planned?	
	IM.MIL3.4	Are risks related to the performance of planned incident management activities identified, analyzed, disposed of, monitored, and controlled?	PM-4 PM-9 PM-11
	IM.MIL4.1	Are incident management activities periodically reviewed and measured to ensure they are effective and producing intended results?	CA-2 CA-7 CP-2 IR-8 PE-3 PL-2 SI-3 SI-4 PM-6 PM-14
	IM.MIL4.2	Are incident management activities periodically reviewed to ensure they are adhering to the plan?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	IM.MIL4.3	Is higher-level management aware of issues related to the performance of incident management?	AC-21 CA-7 SI-4
	IM.MIL5.1	Has the organization adopted a standard definition of incident management activities from which operating units can derive practices that fit their unique operating circumstances?	
	IM.MIL5.2	Are improvements to incident management activities documented and shared across the organization?	
Service Continuity Management			

Subject	CRR Number	CRR Control Description	NIST 800.53
		1. Service continuity plans for high-value services are developed.	
	SCM.1.1	Are service continuity plans developed and documented for assets required for delivery of the critical service?	CP-2 IR-8
		People	CP-2 IR-8
		Information	CP-2 IR-8
		Technology	CP-2 IR-8
		Facilities	CP-2 IR-8
	SCM.1.2	Are service continuity plans developed using established standards, guidelines, and templates?	CP-2 IR-8
	SCM.1.3	Are staff members assigned to execute specific service continuity plans?	CP-2 CP-3 IR-3 IR-8
	SCM.1.4	Are key contacts identified in the service continuity plans?	CP-2 IR-4 IR-8
	SCM.1.5	Are service continuity plans stored in a controlled manner and available to all those who need to know?	CP-2 IR-8
	SCM.1.6	Are availability requirements such as recovery time objectives and recovery point objectives established?	CP-2 IR-8
		2. Service continuity plans are reviewed to resolve conflicts between plans.	
	SCM.2.1	Are plans reviewed to identify and resolve conflicts?	CP-2 IR-8
		3. Service continuity plans are tested to ensure they meet their stated objectives.	
	SCM.3.1	Have standards for testing service continuity plans been implemented?	CP-4 IR-3 PM-14
	SCM.3.2	Has a schedule for testing service continuity plans been established?	CP-4 IR-3 PM-14
	SCM.3.3	Are service continuity plans tested?	CP-4 IR-3 PM-14
	SCM.3.4	Are backup and storage procedures for high-value information assets tested?	CP-4 CP-6 CP-9
	SCM.3.5	Are test results compared with test objectives to identify needed improvements to service continuity plans?	CP-4 IR-3 PM-14
		4. Service continuity plans are executed and reviewed	
	SCM.4.1	Have conditions been identified that trigger the execution of the service continuity plan?	CP-2 CP-10 IR-4 IR-8
	SCM.4.2	Is execution of service continuity plans reviewed?	CP-2 IR-8
	SCM.4.3	Are improvements identified as result of executing service continuity plans?	CP-2 IR-4 IR-8
		Maturity Indicator Level	
	SCM.MIL2.1	Is there a documented plan for performing service continuity activities?	CP-2 IR-8
	SCM.MIL2.2	Is there a documented policy for service continuity?	
	SCM.MIL2.3	Have stakeholders for service continuity activities been identified and made aware of their roles?	CP-2 PS-7 PM-1 PM-11

Subject	CRR Number	CRR Control Description	NIST 800.53
	SCM.MIL2.4	Have service continuity standards and guidelines been identified and implemented?	CP-2 IR-8
	SCM.MIL3.1	Is there management oversight of the performance of the service continuity activities?	AC-21 CA-7 SI-4
	SCM.MIL3.2	Have qualified staff been assigned to perform service continuity activities as planned?	
	SCM.MIL3.3	Is there adequate funding to perform service continuity activities as planned?	
	SCM.MIL3.4	Are risks related to the performance of planned service continuity activities identified, analyzed, disposed of, monitored, and controlled?	PM-4 PM-9 PM-11
	SCM.MIL4.1	Are service continuity activities periodically reviewed and measured to ensure they are effective and producing intended results?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	SCM.MIL4.2	Are service continuity activities periodically reviewed to ensure they are adhering to the plan?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	SCM.MIL4.3	Is higher-level management aware of issues related to the performance of service continuity?	AC-21 CA-7 SI-4
	SCM.MIL5.1	Has the organization adopted a standard definition of service continuity activities from which operating units can derive practices that fit their unique operating circumstances?	
	SCM.MIL5.2	Are improvements to service continuity documented and shared across the organization?	
Risk Management			
		1. A strategy for identifying, analyzing, and mitigating risks is developed.	
	RM.1.1	Have sources of risk that can affect operations been identified?	
	RM.1.2	Have categories been established for risks?	
	RM.1.3	Has a plan for managing operational risk been established?	PM-9 PM-11
	RM.1.4	Is the plan for managing operational risk communicated to stakeholders?	PM-9
		2. Risk tolerance are identified, and the focus of risk management activities is established	
	RM.2.1	Have impact areas been identified, such as reputation, financial health, and regulatory compliance?	RA-2 RA-3 SA-14 PM-9 PM-11
	RM.2.2	Have impact areas been prioritized to determine their relative importance?	RA-2 RA-3 SA-14 PM-9 PM-11
	RM.2.3	Have risk tolerance parameters been established for each impact area?	SA-14 PM-8 PM-9 PM-11
	RM.2.4	Are risk tolerance thresholds, which trigger action, defined for each category of risk?	SA-14 PM-8 PM-9 PM-11
		3. Risks are identified	

Subject	CRR Number	CRR Control Description	NIST 800.53
	RM.3.1	Are operational risks that could affect delivery of the critical service identified?	SA-2 SA-3 PM-16
		4. Risks are analyzed and assigned a disposition	
	RM.4.1	Are risks analyzed to determine potential impact to the critical service?	RA-2 RA-3 SA-14 PM-9 PM-11
	RM.4.2	Is a disposition (accept, transfer, mitigate, etc.) assigned to identified risks?	PM-4 PM-9
		5. Risks to assets and services are mitigated and controlled	
	RM.5.1	Are plans developed for risks that the organization decides to mitigate?	PM-4 PM-9
	RM.5.2	Are identified risks tracked to closure?	PM-4 PM-9
		Maturity Indicator Level	
	RM.MIL2.1	Is there a documented plan for performing risk management activities?	PM-9
	RM.MIL2.2	Is there a documented policy for risk management?	
	RM.MIL2.3	Have stakeholders for risk management activities been identified and made aware of their roles?	CP-2 PS-7 PM-1 PM-11
	RM.MIL2.4	Have risk management activities standards and guidelines been identified and implemented?	PM-9
	RM.MIL3.1	Is there management oversight of the performance of the risk management activities?	AC-21 CA-7 SI-4
	RM.MIL3.2	Have qualified staff been assigned to perform risk management activities as planned?	
	RM.MIL3.3	Is there adequate funding to perform risk management activities as planned?	
	RM.MIL3.4	Are risks related to the performance of planned risk management activities identified, analyzed, disposed of, monitored, and controlled?	PM-4 PM-9 PM-11
	RM.MIL4.1	Are risk management activities periodically reviewed and measured to ensure they are effective and producing intended results?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	RM.MIL4.2	Are risk management activities periodically reviewed to ensure they are adhering to the plan?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	RM.MIL4.3	Is higher-level management aware of issues related to the performance of risk management?	AC-21 CA-7 SI-4
	RM.MIL5.1	Has the organization adopted a standard definition of risk management activities from which operating units can derive practices that fit their unique operating circumstances?	
	RM.MIL5.2	Are improvements to risk management documented and shared across the organization?	
External Dependencies Management			
		1. External dependencies are identified and prioritized to ensure sustained operation of high-value services.	

Subject	CRR Number	CRR Control Description	NIST 800.53
	EDM.1.1	Are dependencies on external relationships that are critical to the service identified?	CP-8 PE-9 PE-11 SA-14 PM-8
	EDM.1.2	Has a process been established for creating and maintaining a list of external dependencies?	CP-8 PE-9 PE-11 SA-14 PM-8
	EDM.1.3	Are external dependencies prioritized?	CP-8 PE-9 PE-11 SA-14 PM-8
		2. Risks due to external dependencies are identified and managed.	
	EDM.2.1	Are risks due to external dependencies identified and managed?	CP-2 SA-2 SA-3 SA-12 PM-16
		3. Relationships with external entities are formally established and maintained.	
	EDM.3.1	Have resilience requirements of the critical service been established that apply specifically to each external dependency?	CP-2 SA-12
	EDM.3.2	Are these requirements reviewed and updated?	CP-2 SA-12
	EDM.3.3	Is the ability of external entities to meet resilience requirements of the critical service considered in the selection process?	CP-2 CP-8 PE-9 PE-11 SA-12 SA-14 PM-8
	EDM.3.4	Are resilience requirements included in formal agreements with external entities?	CP-2 PS-7 SA-9 SA-12
		4. Performance of external entities is managed.	
	EDM.4.1	Is the performance of external entities monitored against resilience requirements?	CP-2 PS-7 SA-4 SA-9 SA-12 SI-4
	EDM.4.2	Has responsibility been assigned for monitoring external entity performance (as related to resilience requirements)?	CP-2 PS-7 SA-12 PM-11
	EDM.4.3	Are corrective actions taken as necessary to address issues with external entity performance (as related to resilience requirements)?	CP-2 SA-12
	EDM.4.4	Are corrective actions evaluated to ensure issues are remedied?	CP-2 SA-12
		5. Dependencies on public services and infrastructure service providers are identified.	
	EDM.5.1	Are public services on which the critical service depends (fire response and rescue services, law enforcement, etc.) identified?	CP-8 PE-9 PE-11 SA-14 PM-8
	EDM.5.2	Are infrastructure providers on which the critical service depends (telecommunications and telephone services, energy sources, etc.) identified?	CP-8 PE-9 PE-11 SA-14 PM-8
		Maturity Indicator Level	
	EDM.MIL2.1	Is there a documented plan for performing external dependency management activities?	

Subject	CRR Number	CRR Control Description	NIST 800.53
	EDM.MIL2.2	Is there a documented policy for external dependency management?	
	EDM.MIL2.3	Have stakeholders for external dependency management activities been identified and made aware of their roles?	CP-2 PS-7 PM-1 PM-11
	EDM.MIL2.4	Have external dependency management activities standards and guidelines been identified and implemented?	
	EDM.MIL3.1	Is there management oversight of the performance of the external dependency management activities?	AC-21 CA-7 SI-4
	EDM.MIL3.2	Have qualified staff been assigned to perform external dependency management activities as planned?	
	EDM.MIL3.3	Is there adequate funding to perform external dependency management activities as planned?	
	EDM.MIL3.4	Are risks related to the performance of planned external dependency management activities identified, analyzed, disposed of, monitored, and controlled?	PM-4 PM-9 PM-11
	EDM.MIL4.1	Are external dependency management activities periodically reviewed and measured to ensure they are effective and producing intended results?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	EDM.MIL4.2	Are external dependency management activities periodically reviewed to ensure they are adhering to the plan?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	EDM.MIL4.3	Is higher-level management aware of issues related to external dependency management?	AC-21 CA-7 SI-4
	EDM.MIL5.1	Has the organization adopted a standard definition of the external dependency management activities from which operating units can derive practices that fit their unique operating circumstances?	
	EDM.MIL5.2	Are improvements to external dependency management documented and shared across the organization?	
Training & Awareness			
		1. Cyber security awareness and training programs are established.	
	TA.1.1	Have cyber security awareness needs been identified for the critical service?	AT-2 PM-13
	TA.1.2	Have required skills been identified for specific roles (administrators, technicians, etc.) for the critical service?	AT-2 PM-13
	TA.1.3	Are skill gaps present in personnel responsible for cyber security identified?	AT-2 PM-13
	TA.1.4	Have training needs been identified?	AT-2 PM-13
		2. Awareness and training activities are conducted.	
	TA.2.1	Are cyber security awareness activities for the critical service conducted?	AT-2 PM-13
	TA.2.2	Are cyber security training activities for the critical service conducted?	AT-2 PM-13

Subject	CRR Number	CRR Control Description	NIST 800.53
	TA.2.3	Is the effectiveness of the awareness and training programs evaluated?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	TA.2.4	Are awareness and training activities revised as needed?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	TA.2.5	Have privileged users been trained in their specific roles and responsibilities in support of the critical service?	AT-3 PM-13
	TA.2.6	Have senior executives been trained in their specific roles and responsibilities in support of the critical service?	AT-3 PM-13
	TA.2.7	Have physical and information security personnel been trained in their specific roles and responsibilities in support of the critical service?	AT-3 PM-13
		Maturity Indicator Level	
	TA.MIL2.1	Is there a documented plan for performing training activities?	
	TA.MIL2.2	Is there a documented policy for training?	
	TA.MIL2.3	Have stakeholders for training activities been identified and made aware of their roles?	CP-2 PS-7 PM-1 PM-11
	TA.MIL2.4	Have training standards and guidelines been identified and implemented?	
	TA.MIL3.1	Is there management oversight of the performance of the training activities?	AC-21 CA-7 SI-4
	TA.MIL3.2	Have qualified staff been assigned to perform training activities as planned?	
	TA.MIL3.3	Is there adequate funding to perform training activities as planned?	
	TA.MIL3.4	Are risks related to the performance of planned training activities identified, analyzed, disposed of, monitored, and controlled?	PM-4 PM-9 PM-11
	TA.MIL4.1	Are training activities periodically reviewed and measured to ensure they are effective and producing intended results?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	TA.MIL4.2	Are training activities periodically reviewed to ensure they are adhering to the plan?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	TA.MIL4.3	Is higher-level management aware of issues related to the performance of training?	AC-21 CA-7 SI-4
	TA.MIL5.1	Has the organization adopted a standard definition of the training activities from which operating units can derive practices that fit their unique operating circumstances?	
	TA.MIL5.2	Are improvements to training documented and shared across the organization?	
Situational Awareness			
		1. Threat monitoring is performed.	
	SA.1.1	Has responsibility for monitoring sources of threat information been assigned?	AT-3 SI-5 PM-13 PM-15 PM-16

Subject	CRR Number	CRR Control Description	NIST 800.53
	SA.1.2	Have threat monitoring procedures been implemented?	RA-3 SI-5 PM-12 PM-16
	SA.1.3	Have resources been assigned and trained to perform threat monitoring?	AT-3 PM-13
		2. The requirements for communicating threat information are established.	
	SA.2.1	Have internal stakeholders (such as the critical service owner and incident management staff) been identified to whom threat information must be communicated?	CA-7 SI-4
	SA.2.2	Have external stakeholders (such as emergency management personnel, regulatory, and information sharing organizations) been identified to whom threat information must be communicated?	CA-7 SI-4 SI-5 PM-15
		3. Threat information is communicated.	
	SA.3.1	Is threat information communicated to stakeholders?	CA-7 SI-4 SI-5 PM-15
	SA.3.2	Have resources been assigned authority and accountability for communicating threat information?	AT-3 PM-13
	SA.3.3	Have resources been trained with respect to their specific role in communicating threat information?	AT-2 AT-3 PM-13
		Maturity Indicator Level	
	SA.MIL2.1	Is there a documented plan for performing situational awareness activities?	
	SA.MIL2.2	Is there a documented policy for situational awareness?	
	SA.MIL2.3	Have stakeholders for situational awareness activities been identified and made aware of their roles?	CP-2 PS-7 PM-1 PM-11
	SA.MIL2.4	Have situational awareness standards and guidelines been identified and implemented?	
	SA.MIL3.1	Is there management oversight of the performance of situational awareness activities?	AC-21 CA-7 SI-4
	SA.MIL3.2	Have qualified staff been assigned to perform situational awareness activities as planned?	
	SA.MIL3.3	Is there adequate funding to perform situational awareness activities as planned?	
	SA.MIL3.4	Are risks related to the performance of planned situational awareness activities identified, analyzed, disposed of, monitored, and controlled?	PM-4 PM-9 PM-11
	SA.MIL4.1	Are situational awareness activities periodically reviewed and measured to ensure they are effective and producing intended results?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6
	SA.MIL4.2	Are situational awareness activities periodically reviewed to ensure they are adhering to the plan?	CA-2 CA-7 CP-2 IR-8 PL-2 PM-6

Subject	CRR Number	CRR Control Description	NIST 800.53
	SA.MIL4.3	Is higher-level management aware of issues related to situational awareness?	AC-21 CA-7 SI-4
	SA.MIL5.1	Has the organization adopted a standard definition of the situational awareness activities from which operating units can derive practices that fit their unique operating circumstances?	
	SA.MIL5.2	Are improvements to situational awareness activities documented and shared across the organization?	

End of Document

ATTACHMENT F
INFORMATION TECHNOLOGY USAGE

SEE SEPARATE ATTACHMENT TITLED
“INFORMATION TECHNOLOGY USAGE”

INFORMATION TECHNOLOGY USAGE POLICY

COUNTY OF ORANGE

1 INTRODUCTION:

The County of Orange Information Technology (IT) Usage Policy is the foundation of the County's information security efforts. Each member of the County workforce is responsible for understanding his/her role in maintaining County IT security. This policy summarizes your information technology responsibilities. To learn more about information security, please see the Information Technology Security Policy.

Complete **Section 5: Acknowledgement** after you have finished reading this document. Your signature on the Acknowledgement indicates that you understand and will comply with County security policy. If you disregard security policies, standards, or procedures, you can be subject to County and agency-specific disciplinary action.

2 TERMS YOU NEED TO KNOW:

Authentication
The process of verifying the identity of anyone who wants to use County information before granting them access.

Back Up
To copy files to a second medium (for example, a disk or tape) as a precaution in case the first medium fails.

Confidentiality / Non-Disclosure Agreement
An agreement that outlines sensitive materials or knowledge that two or more parties wish to share with one another. By way of such agreement, the parties to the agreement agree not to share or discuss with outside parties the information covered by the agreement.

System or Software Configuration Files
Highly important files that control the operation of entire systems or software.

Electronic Communication
Messages sent and received electronically through any electronic text or voice transfer/storage system. This includes e-mail, text messages, instant messages (IM) and voicemail.

Encryption
The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain tex*t; encrypted data is referred to as *cipher text*.

Information Security
Safeguarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.

Information Technology (IT)
The broad subject concerned with all aspects of managing and processing information within an organization.

Local Security Administrator (LSA)
The person at each agency who is responsible for the operational maintenance of IT security resources within the agency.

Network
Two or more linked computer systems. There are many different types of computer networks.

Password
Sequence of characters (letters, numbers, symbols) used in combination with a User ID to access a computer system or network. Passwords are used to authenticate the user before s/he gains access to the system.

Personally Identifiable Information (PII) Any piece of information that could be used to uniquely identify, contact, or locate a single person. Examples include: full name; national identification number; email address; IP address; driver's license number; and Social Security Number.

User Any individual who uses a computer.

User ID Unique name given to a user for identification to a computer or telephone network, database, application, etc. Coupled with a password, it provides a minimal level of security.

Virus / Malicious Software A software program that interferes with computer operation, damages or destroys electronic data, or spreads itself to other computers. Viruses and malicious software are often transmitted via email, documents attached to email, and the Internet.

Workforce Member Any member of the County workforce, including employees, temporary help, contractors, vendors and volunteers.

3 POLICY OVERVIEW

As a member of the County workforce, you are expected to comply with the County's Information Technology Usage Policy. Your agency may have additional policies that you must follow as part of your job.

The following are key concepts of the County's policy:

- Information created or used in support of County business activities is the property of the County.
- Your assigned information technology resources are meant to facilitate the efficient and effective performance of your duties. It is your responsibility to ensure that resources are not misused and that you comply with policy.
- If you need to access confidential information as part of your duties, you will be asked to sign a confidentiality or non-disclosure agreement before you access the County network.
- Many County facilities house sensitive or critical information systems. You are expected to comply with all physical access controls designed to restrict unauthorized access.
- You may not remove County equipment or data in any format from the workplace unless you have received prior written approval from your supervisor or manager.
- The use of the network and Internet is a privilege, not a right. If you violate policy, you may lose your network and/or Internet access. The County may refuse to reinstate your access for the remainder of your employment at the County. The County may also take other disciplinary action as appropriate under County policy, departmental policy and applicable employment MOUs.

4 YOUR RESPONSIBILITIES

Your security responsibilities fall under several different Information Technology categories. Each category and the key responsibilities associated with it are listed below:

USER IDs AND PASSWORDS

- You will be issued a network user ID unique to you. Only you may use your user ID to access County resources (e.g. computer, telephone, FAX).
- You will be issued a default password at the same time as your user ID. You will be prompted to change your password the first time you log in to the system.
- Do not share user IDs and passwords with other users or individuals, including coworkers and supervisors. Treat your password as sensitive and highly confidential information.
- You are agreeing to follow the Information Technology Usage Policy when you accept a password from the County and use it to access the County data or telephone networks, the Internet, or the Intranet.
- Change your password immediately if you think someone else knows it. Report your suspicions to management.
- If you lose or forget your password, you are required to request a password reset. No one else can do it for you.

HARDWARE AND SOFTWARE

- The County will provide, and employees may request, peripheral equipment such as ear buds for cellular phones or Blackberry devices, as may be necessary to enable compliance with all local laws which pertain to the use of mobile communication equipment or the individual workplace needs for the employee to perform his or her employment.
- Never download or install any hardware or software without prior written approval of your agency IT representative.
- Do not make any changes to system and/or software configuration files unless specifically authorized in writing by your agency IT.
- Maintain your business data files on a network (or “shared”) drive so that they can be backed up according to your agency’s regular backup schedule.
- Use the “lock workstation” feature any time you leave your workstation logged on to the network and you are away from your desk.
- Do not connect a County laptop or other mobile device to the network until it has been scanned for viruses and malicious software.
- Follow the authentication procedures defined by your agency whenever you log in to the County network via Remote Access.
- Do not attempt to connect your workstation, laptop, or other computing device to the Internet via an unauthorized wireless or other connection while simultaneously connected to any County network.
- Retain original software installed on your computer if it is provided to you. The software must be available when your system is serviced in case it needs to be reinstalled.
- Do not keep liquids or magnets on or near computers, as they can cause serious damage.
- Ensure that your equipment is plugged into a surge protector at all times.

- Report all computer problems in detail on the appropriate form and/or when you contact the County Service Desk or discuss the problem with your agency's Help Desk.

- Report equipment damage immediately to the County Service Desk or your agency's Help Desk.

EMAIL and TELEPHONE

- The e-mail and telephone systems and networks are primarily for official County business.

- Management can freely inspect or review electronic mail and data files including voicemail. Employees should have no expectation of privacy regarding their internet usage, electronic mail or any other use of County computing or telephone equipment.

- Do not use a County email account or voicemail box assigned to another individual to send or receive messages unless you have been authorized, in writing, to act as that individual's delegate.

- Use of personal Internet (external) email systems from County networks and/or desktop devices is prohibited unless there is a compelling business reason for such use and prior written approval has been given by agency management and agency IT.

- Do not configure or use automated forwarding to send County email to Internet-based (external) email systems unless specifically authorized to do so, in writing, by County management.

- Send confidential information via email only with the written permission of management and only via an approved method. Mark the email according to agency policy.

- Treat confidential or restricted files sent as attachments to email messages as confidential or restricted documents. This also applies to confidential or restricted information embedded within an email message as message text or a voicemail message.

- Do not delete email or voicemail messages or other data if management has identified the subject matter as relevant to pending or anticipated litigation, personnel investigation, or other legal processes.

THE INTERNET / INTRANET

- Internet/Intranet access is primarily for County business.

- You may access the Internet for limited personal use only during nonworking time and in strict compliance with policy. If there is any doubt about whether an activity is appropriate, consult with your Department Head or his/her designee.

INFORMATION SECURITY

- Treat hardcopy or electronic Personally Identifiable Information (PII) as confidential and take all precautions necessary to ensure that it is not compromised. Intentional – or even accidental – disclosure of PII to unauthorized users is a violation of policy.

- Don't leave PII unattended or unsecured for any period of time.

- Be sure to follow your agency's policy for disposing of confidential data. This may include the physical destruction of data through shredding or other methods.

- Information created, sent, stored or received via the email system, network, Internet, telephones (including voicemail), fax or the Intranet is the property of the County.

- Do not expect information you create and store on County systems, including email messages or electronic files, to be private. Encrypting or using other measures to protect or “lock” an email message or an electronic file does not mean that the data are private.
- The County reserves the right to, at any time and without notice, access, read and review, monitor, and copy all messages and files on its computer system as it deems necessary.
- The County may disclose text or images to law enforcement without your consent as necessary.

PROHIBITED ACTIVITY

Unless you are specifically authorized by your manager or agency in writing, the following uses are prohibited by the Information Technology Security Policy:

- Using, transmitting, or seeking inappropriate or offensive materials, including but not limited to vulgar, profane, obscene, abusive, harassing, belligerent, threatening, or defamatory (harming another's reputation by lies) language or materials.
- Accessing, attempting to access, or encouraging others to access controversial or offensive materials.
- Revealing PII without permission, such as another's home address, telephone number, credit card number or Social Security Number.
- Making offensive or harassing statements or jokes about language, race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.
- Sending or soliciting sexually oriented messages, images, video or sound files.
- Visiting sites featuring pornography, terrorism, espionage, theft, drugs or other subjects that violate or encourage violation of the law.
- Gambling or engaging in any other activity in violation of local, state, or federal law.
- Uses or activities that violate the law or County policy or encourage others to violate the law or County policy. These include:
    - Accessing, transmitting, or seeking confidential information about clients or coworkers without proper authorization.
    - Intruding, or trying to intrude, into the folders, files, work, networks, or computers of others, or intercepting communications intended for others.
    - Knowingly downloading or transmitting confidential information without proper authorization.
- Uses that cause harm to others or damage to their property, including but not limited to:
    - Downloading or transmitting copyrighted materials without the permission of the copyright owner. Even if materials on the network or the Internet are not marked with the copyright symbol, ©, assume that they are protected under copyright law.
    - Using someone else’s password to access the network or the Internet.
    - Impersonating another user or misleading message recipients into believing that someone other than the authenticated user is communicating a message.

  - Uploading a virus, other harmful component, or corrupted data or vandalizing any part of the network.
  - Creating, executing, forwarding, or introducing computer code designed to self-replicate, damage, or impede the performance of any computer's memory, storage, operating system, application software, or any other functionality.
  - Engaging in activities that jeopardize the security of and access to the County network or other networks on the Internet.

- Downloading or using any software on the network other than that licensed or approved by the County.

- Conducting unauthorized business or commercial activities including, but not limited to:

  - Buying or selling anything over the Internet.
  - Soliciting or advertising the sale of any goods or services.
  - Unauthorized outside fund-raising activities, participation in any lobbying activity, or engaging in any prohibited partisan political activity.
  - Posting County, department and/or other public agency information to external news agencies, service bureaus, social networking sites, message boards, blogs or other forums.

- Uses that waste resources, including, but not limited to:

  - Printing of personal files.
  - Sending chain letters for any reason.
  - Including unnecessary recipients on an email. Only copy others on an email or voicemail message who should be "in the loop" on the topic addressed.
  - Indiscriminate use of distribution lists. Before using a distribution list, determine whether or not it is appropriate for everyone on that list to receive the email.
  - "All hands" emails. Emails of this type are to be sent only after management permission has been obtained.

5 ACKNOWLEDGEMENT

- If you violate security policies, standards, or procedures, you can be subject to County and agency-specific disciplinary action up to and including discharge.

By signing this document, I acknowledge that I have read, understand and will comply with this County of Orange Information Technology Usage Policy. I understand that the complete Information Technology Usage Policy is available for me to review on the County's intranet. I also may request a copy from the County Service Desk, my agency's Help Desk, or my agency's Local Security Administrator.

Workforce Member Name (please print): ____

Workforce Member Signature: ____

Agency/Department: ____

Date: ____________________

ATTACHMENT G
IT SECURITY POLICY 2009

SEE SEPARATE ATTACHMENT TITLED
"IT SECURITY POLICY 2009"

Revision History

Date	Revision Scope	Author	Description
12/31/07	All Sections	CEO/IT, ISO	Document creation.
02/21/08	All Sections	CEO/IT, ISO	Document submitted for peer review.
03/10/08	All Sections	CEO/IT	Integration of document revisions.
03/13/08	All Sections	CEO/IT	Integration of document revisions from SWG meeting held 03/13/08.
03/14/08	All Sections	CEO/IT, ISO	Integration of document revisions from meeting with Senior Management held 03/14/08.
03/17/08	All Sections	CEO/IT	Integration of document revisions from SWG meeting held 03/13/08 and HR meeting held 03/17/08.
03/19/08	All Sections	CEO/IT	Integration of document revisions from SWG meeting held 03/18/08.
03/25/08	All Sections	CEO/IT	Integration of document revisions from SWG meeting held 03/13/08, 03/18/08 & 03/24/08; Senior Management meeting held 03/14/08.
04/09/08	Added Appendix, Added Comments	CEO/IT	Added Policy Statement Source Matrix. Added comments for Technology Council Review showing those areas of concern.
06/19/08	Sections 1.3,1.4, 6.2.22	Technology Council	Agency Department Head Signs Approval, forward to CIO for Review and Comment. Use CERT process for Level 4 incident handling.
07/09/08	All Sections	CEO/IT	Corrections to minor typographical/grammatical and formatting errors
07/09/08	Section 2.2.7	CEO/IT	Change requirement that all workforce members read all documents related to County IT security to requirement to read, accept and comply with Workforce Member Usage Agreement.
07/09/08	Section 1.4.1 Section 6.2.18 Section 7.2	CEO/IT	Integration of revisions suggested by SWG Team members.
12/1/08	Section 2.1	CEO/IT	Update to match approved governance diagram
9/15/09	All Sections	CEO/HR	Completed Bargaining unit review and approval

Policy Approval

We have approved this Information Technology Security Policy as reasonably designed to enable the County of Orange and County agencies/departments to address their security obligations for County information assets.

(Signed copy on file in CIO Office)
Satish Ajmani
Deputy CEO/Chief Information Officer

(Signed copy on file in CIO Office)
Tony Lucich
County Information Security Officer

Table of Contents

1 INTRODUCTION

Information technology is a critical component of all primary County business processes. The County's visibility on the Internet, the increased use of electronic communication, and a dependence on information technology resources requires the development, maintenance and dissemination of a set of common IT security policies designed to protect these assets.

Security threats, such as identity theft, viruses, and phishing have been increasing both in frequency and in complexity. Due to these increasing security threats, a common set of safeguards is required to minimize the risk, cost and duration of any level of disruption to the County's business processes in the event of damage to or failure, loss, corruption, or discontinuation of a strategic component of its critical IT infrastructure. Ensuring such an environment requires an enterprise approach to security that:

- Promotes an enterprise view among all County agencies/departments
- Recognizes an interdependent relationship among County agencies and/or departments
- Requires adherence to a common, minimum security architecture and related standards, guidelines and procedures

Effective security is a civic responsibility and a team effort involving the participation and support of every County agency, employee and affiliate that deals with information and/or information systems. To further this enterprise-wide responsibility, previously published security-related policies have been consolidated into this IT Security Policy. This document supersedes all prior Countywide IT security polices. This document provides a comprehensive Information Technology Security Policy for County agencies.

It is the responsibility of every County employee and affiliate to know, understand, and adhere to the policy, procedures, standards, and guidelines contained herein and to conduct their activities accordingly. This policy statement has been adopted in order to provide guidance and protection to County employees and to safeguard the information resources entrusted to those employees. Information security policies raise user awareness of the potential risks associated with information technology. Employee awareness through dissemination of policy helps minimize the cost of security incidents; accelerate the development of new application systems; and assure the consistent implementation of controls for information systems throughout the organization.

County information security policy is based upon the ISO 27002:2005 standards, the NIST standards, and Best Practices. The policy is designed to comply with applicable laws and regulations; however, if there is a conflict, applicable laws and regulations will take precedence. The policy statements are to be considered minimum requirements for providing a secure environment for the development, implementation, and support of information technology and systems. Agencies may develop detailed policies and procedures to handle agency-specific cases.

The enterprise security policy and standards established under the authority described herein are resources intended to assist County agencies and/or departments to more effectively manage the information technology resources.

1.1 AUTHORITY

The authority to set technology policy for all agencies is derived from the County IT Strategic Plan. The IT Security Policy was developed in conjunction with the security guiding principles along with the governance and compliance goals set forth in the County IT Strategic Plan. The IT Governance Model, discussed below, executes this plan by facilitating change agreement for the IT Security Policy. The County IT Strategic Plan states *"The County will adhere to an agreed-upon minimum set of security/privacy controls."* as this supports countywide strategic priorities. Supporting the foundational principle of *"driving towards the use of common IT components"*, the County IT Strategic Plan states *"The County will have an agreed-upon baseline set of security monitoring and incident response policies."*

1.2 IT GOVERNANCE MODEL

IT governance consists of leadership, stakeholder engagement, and collaboration processes that ensure that the County's IT investments support overall business strategies and policy objectives. IT governance facilitates general agreement on IT policies, resources, and architecture.

The Technology Council receives input from multiple Architecture Groups and Working Groups, including the Technology Architecture Group (TAG) and the Security Working Group (SWG). Changes or updates to this policy may be proposed by any Architecture Group or Working Group. The SWG works collaboratively with the ISO to make recommendations to the Technology Council and the Business Council through the governance process. The SWG also advises the office of the CIO and Technology Council as appropriate. As needed, proposals will be forwarded to the Technology Council and Business Council for review and approval. The Technology Council is responsible for reviewing and recommending IT guiding principles, standards, policies, and guidelines to the CIO. The Business Council is responsible for approving IT guiding principles, standards, policies, and guidelines proposed by the CIO and/or Technology Council.

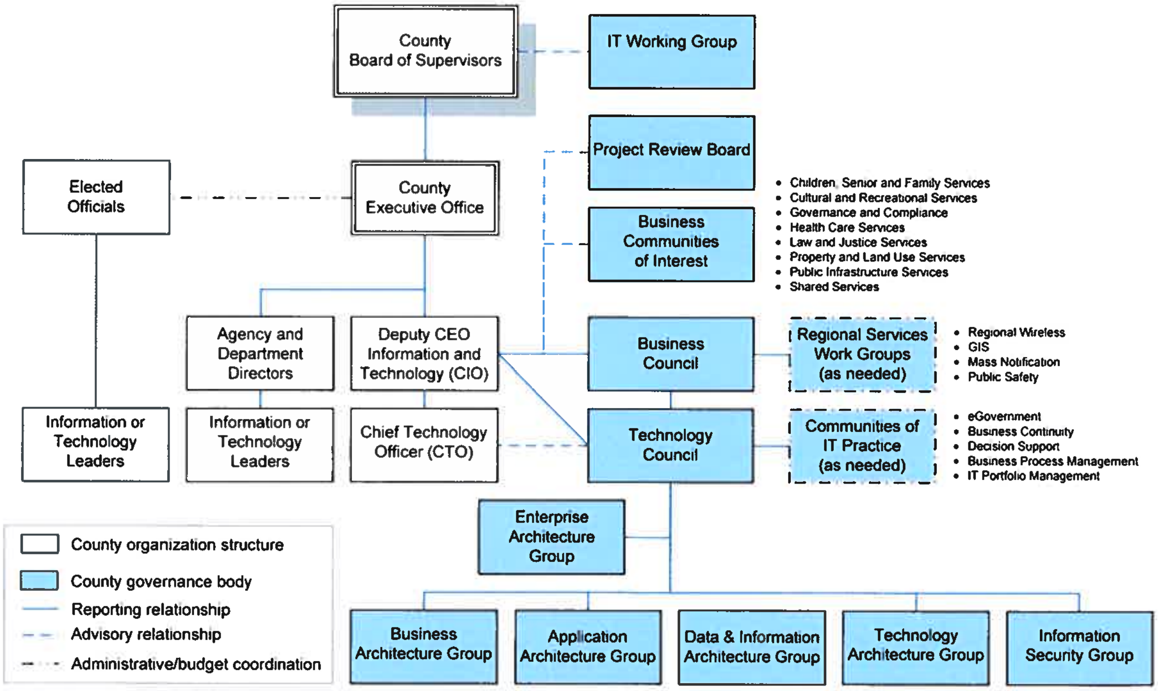

County Board of Supervisors
IT Working Group
Project Review Board
Elected Officials
County Executive Office
Business Communities of Interest
• Children, Senior and Family Services
• Cultural and Recreational Services
• Governance and Compliance
• Health Care Services
• Law and Justice Services
• Property and Land Use Services
• Public Infrastructure Services
• Shared Services
Agency and Department Directors
Deputy CEO Information and Technology (CIO)
Business Council
Regional Services Work Groups (as needed)
• Regional Wireless
• GIS
• Mass Notification
• Public Safety
Information or Technology Leaders
Information or Technology Leaders
Chief Technology Officer (CTO)
Technology Council
Communities of IT Practice (as needed)
• eGovernment
• Business Continuity
• Decision Support
• Business Process Management
• IT Portfolio Management
Enterprise Architecture Group
County organization structure
County governance body
Reporting relationship
Advisory relationship
Administrative/budget coordination
Business Architecture Group
Application Architecture Group
Data & Information Architecture Group
Technology Architecture Group
Information Security Group

Fig. 1: **County IT Governance Model**

1.3 ENFORCEMENT

Individual County agencies and/or departments will be responsible for developing an IT Security Plan including detailed procedures to comply with this policy. Each agency IT Manager will create a Security Plan based on this framework guideline that this meets the intent and submit to their Agency Director for signature approval. Agencies will submit their approved IT Security Plans to the CIO for review and comment. (Please see Exceptions section for more information.)

The IT Security Policy will guide periodic security reviews as well as audits by the Internal Audit Department. In addition, the County will review applicable equipment and service purchases to ensure that vendors and contractors are aware of policy and are in compliance with it. Violators of policy may be subject to employee disciplinary procedures. Agencies may impose sanctions upon their employees for violations of policy and standards. All disciplinary actions and/or sections must be in compliance with applicable Human Resources policy.

1.4 EXCEPTIONS

Agencies will document the need for exceptions to this policy, including the scope and extent of the exception; the safeguards to be implemented to mitigate risks; the specific timeframe for the exception; and evidence of management approval of the exception.

The policy described in this document is applicable to production-level systems. Internal test and experimental systems not connected to a production network do not require the same level of security unless they make use of confidential information.

Application development systems may also be exempt provided they are on a network that is physically separated or suitably isolated from production networks. However, if development or test systems are on the same physical or virtual network as production systems or contain confidential information, they must follow the same security policy as production systems.

1.4.1 HIPAA

While they address similar topics, the County Health Insurance Portability and Accountability Act (HIPAA) Policies and the IT Security Policy function as separate policies. The IT Security Policy is more comprehensive in scope as compared with the HIPAA Policy. The HIPAA Policy establishes County policy pursuant to federal HIPAA security requirements for use of electronic protected health information (ePHI) by the County and designated health care entities.

ePHI is also addressed within the IT Security Policy. If a conflict exists between this policy and the HIPAA Policy, the HIPAA Policy will prevail. The County HIPAA Security Policy is available at:
http://intra2k3.ocgov.com/cota/policies/brd_of_supervisors.asp

1.5 IT SECURITY PROGRAM IMPLEMENTATION PROCESS

The County Board of Supervisors approved the CIO to develop a comprehensive security program. This security program is based on the County IT Strategic Plan. The following diagram illustrates the process being used to define and implement the County's information security program.

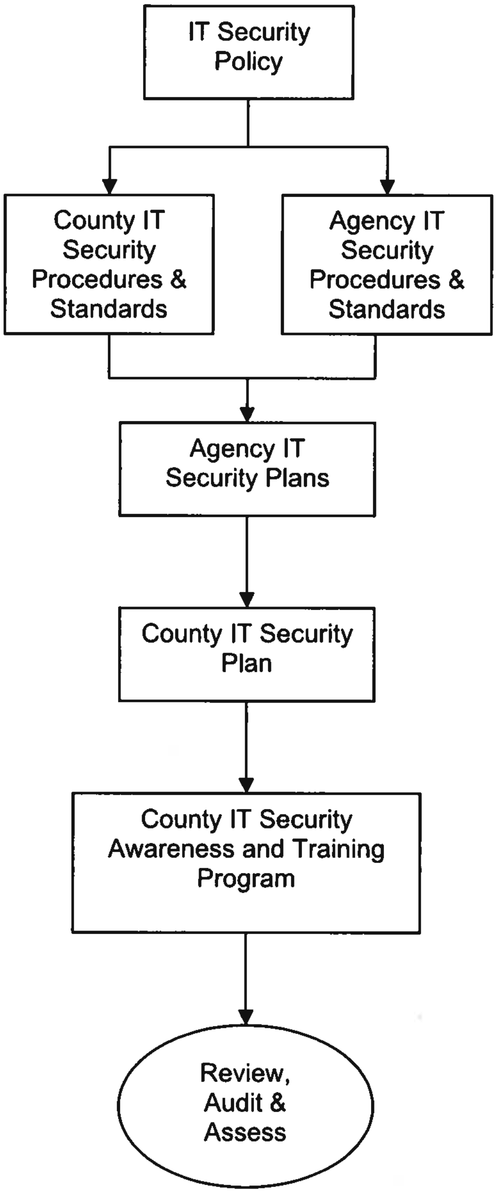

IT Security Policy
County IT Security Procedures & Standards
Agency IT Security Procedures & Standards
Agency IT Security Plans
County IT Security Plan
County IT Security Awareness and Training Program
Review, Audit & Assess

Fig. 2: **County IT Security Program Implementation Process**

1.6 SCOPE/LIMITATIONS

This policy applies to all agencies in the County as well as all employees, contractors, vendors, customers, and others who utilize, possess or have access to County IT resources.

2 INFORMATION TECHNOLOGY SECURITY

2.1 PURPOSE

The purpose of this document is to define a common security environment within the County to:

- Foster system security and availability
- Ensure data integrity and confidentiality, and
- Encourage the prevention of unauthorized access or damage to, or misuse or loss of, County IT assets and/or data

2.2 POLICY STATEMENT

2.2.1 All information that is created or used within the County's trusted environment in support of County business activities shall be considered the property of the County. All County property should be used in compliance with the IT Security Policy.

2.2.2 County information is a valuable asset and must be protected from unauthorized disclosure, modification, or destruction. Prudent information security standards and practices must be implemented to ensure that the integrity, confidentiality, and availability of County information are not compromised. All County information shall be protected from the time of its creation through its useful life and authorized disposal.

2.2.3 The County shall be responsible for the policy defined in this document. An independent annual review of County Information Security control objectives, policy and procedures shall be completed by a resource identified by the Chief Information Officer (CIO).

2.2.4 County information technology resources are provided to authorized users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations on users and is subject to County policy and applicable state and federal laws. It is the responsibility of users to ensure that resources are not misused and that they comply with policy.

2.2.5 This policy provides a minimal security framework for the County and each individual agency. In the event that an agency does not have or maintain its own IT security policy, the agency should, at a minimum, adopt and adhere to this policy.

2.2.6 Agencies contracting with business partners, such as contractors, consultants or vendors, shall use IT policy guidelines provided and approved by the CIO and County Council (COCO) to ensure the safeguarding of County information systems. These contracts must be reviewed for appropriate compliance with County Business Continuity and IT Security Policies.

2.2.7 Each agency shall ensure that all County workforce members within its organization read, accept and comply with the IT Security Policy Workforce Member Usage Agreement.

2.2.8 Each agency shall ensure that all software used on County systems and in the execution of County business shall be used legally and in compliance with licensing agreements.

2.2.9 Each agency shall ensure that all County workforce members within its organization, including employees, contractors, and consultants, receive appropriate training in IT security. IT security training is to be conducted on an annual basis.

2.3 RELATED POLICY

- Agency policy as applicable.

3 ORGANIZATIONAL SECURITY

3.1 PURPOSE

Organizational Security is intended to facilitate information security within an organization through the implementation of an information security infrastructure. An information security infrastructure is the complete set of information security-related systems, procedures, policies and physical implementations of information security administration.

Organizational Security specifically applies to any situation in which a County agency uses resources from a vendor or contractor to access and perform work with County information systems.

3.2 POLICY STATEMENT

3.2.1 The primary function of the Security Working Group (SWG) is to bring together representatives from different parts of the organization with relevant security roles and job functions for the purpose of collaboratively establishing information security strategies for selected IT initiatives. The SWG advises the office of the CIO and the Technology Council as appropriate.

3.2.2 Each agency should identify an Information Security Officer (ISO), responsible for management of information security issues for that agency. Each agency decides which appropriate qualifications and criteria are to be used for selection of an ISO.

3.2.3 All agencies should clearly define information security responsibilities in the following areas (at a minimum):

- Information Security Management
- Information Classification
- Risk Assessment
- Compliance
- Business Continuity/Disaster Recovery
- Software Development Oversight
- Incident Response
- Security Awareness/Training.

3.2.4 All agencies shall consult with the ISO when developing new information processing facilities, applications and access methods to ensure consistency with existing and anticipated IT security policies.

3.2.5 Employees who need to access confidential information are required to sign confidentiality and/or non-disclosure agreements when initially hired. External users (contractors, vendors and customers) who are not already covered by an existing agreement should also sign such agreements prior to being given access to confidential information. Confidentiality and non-disclosure agreements should be reviewed regularly, especially when employees leave the organization or when contracts expire.

3.2.6 Risk assessment and identification should take place prior to establishing vendor, customer or contractor access to County information systems and must be in accordance with the policy set forth in this document (see Section 7: Access Control).

3.2.7 Contractors and vendors who have access to Personal Identifiable Information, as defined herein, shall comply with the California Information Practices Act and the Consumer Credit Reporting Act, as applicable.

3.2.8 Any agreement or contract with a vendor, contractor or customer that involves access to County information resources will contain sections that delineate County information security issues relevant to that business access and require the vendor, contractor and/or customer to adhere to County IT Security Policy. If Security is outsourced, the vendor must demonstrate a standard of care as this must also be reflected in the vendor contract.

3.2.9 The office of the CIO shall make experienced resources available to agencies to complete annual reviews of the agency's approach to managing information security and its implementation (e.g. objectives, controls, policies, processes and procedures).

4 HUMAN RESOURCES SECURITY

4.1 PURPOSE

Human Resources Security addresses information security throughout the entire lifecycle of employment, from the recruitment stage, during an individual's employment, and through termination or separation. County workforce members include all employees, contractors, vendors and customers working to forward the County's mission.

Some of the specific purposes of Human Resources Security are to:

- Minimize the risks at the recruitment stage of employment for all potential County workforce members
- Ensure that County workforce members are knowledgeable and aware of security threats, concerns, and the procedures for reporting security incidents
- Ensure that a disciplinary process is in place to deter County workforce members who may disregard security policy and procedures

4.2 POLICY STATEMENT

4.2.1 Based on an employee's role and job responsibilities, agencies must conduct personnel screenings/background checks of prospective employees who will be granted access to County information systems.

4.2.2 All agencies should use terms and conditions of employment to clearly state the employee's responsibilities for information security. Such terms and conditions are typically defined in a non-disclosure or confidentiality agreement that is signed by the employee and maintained by Human Resources. The agreement should also define actions that will be taken in the event of non-compliance.

4.2.3 County and agency-specific disciplinary procedures will be followed for users who disregard security policies, standards and procedures.

4.2.4 Upon termination, separation or applicable job change (including but not limited to moves, adds, transfers, promotions, change of duties, and change in job responsibilities):

- Employee must return all County assets
- Human Resources must notify appropriate IT personnel to update and/or remove employee access rights
- An exit interview is to be conducted and must include confirmation that all necessary assets and access (both physical and logical) have been returned to the County

4.2.5 Human Resources will provide a list of terminated employees and employee changes to IT on a quarterly basis. Human Resources is responsible for reviewing inactive/unused user account reports as provided by IT and providing updates to IT as appropriate.

4.2.6 Agencies contracting with business partners, such as contractors, consultants or vendors, shall ensure that personnel screenings/background checks are addressed as part of the business relationship.

4.3 RELATED POLICY

- Sections 2.2.10-2.2.12: Security Awareness
- Section 3.2.5: Non-disclosure/Confidentiality Agreements

5 PHYSICAL AND ENVIRONMENTAL SECURITY

5.1 PURPOSE

Physical and Environmental Security is intended to protect County assets from harm caused by physical threats (e.g., civil unrest, sabotage, assault) or environmental events (e.g., earthquake, flood, fire, severe weather). Physical and environmental security measures are used in conjunction with the County Business Continuity Management Policy to protect County assets.

Specific areas addressed in this section are:

- Physical safeguards to the perimeter of agency facilities
- Prevention of unauthorized physical access
- Reduction in risk from environmental threats and hazards
- Protection of business critical equipment and information systems from power anomalies
- Protection of sensitive information assets from improper data cleansing and disposal

5.2 POLICY STATEMENT

5.2.1 Procedures and facility hardening measures shall be adopted to prevent attempts at and detection of unauthorized access or damage to facilities that contain County information systems and/or processing facilities.

5.2.2 Restricted areas within facilities that house sensitive or critical County information systems will, at a minimum, utilize physical access controls designed to permit access by authorized personnel only.

5.2.3 Physical protection measures against damage from external and environmental threats shall be implemented by all agencies as appropriate.

5.2.4 Access to any office, computer room, or work area that contains sensitive information shall be physically restricted from unauthorized access.

5.2.5 Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. An example of this would be separating the two areas by a badge-only accessible door.

5.2.6 Continuity of power should be provided to maintain the availability of critical equipment and information systems.

5.2.7 Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage. Different, yet appropriate methods should be utilized for internal and external cabling.

5.2.8 Equipment should be properly maintained to ensure its continued availability and integrity.

5.2.9 Unless approved by County management, no County computer equipment should be removed from the premises.

5.2.10 Prior to re-deployment, surplus, donation, disposal or destruction of equipment containing storage media, media should be appropriately cleansed to prevent unauthorized exposure of data. NIST standards should be followed for appropriate levels of storage media cleansing.

5.2.11 Disposal of equipment shall be done in accordance with all applicable County, state or federal surplus property and environmental disposal laws, regulations or policies.

5.2.12 All shared IT infrastructure by more than one agency shall meet countywide security policy for facility standards, availability, access, data & network security.

5.3 RELATED POLICY

- County Business Continuity Management Policy

6 SYSTEM AND NETWORK OPERATIONS MANAGEMENT

6.1 PURPOSE

System and Network Operations Management includes the documentation and maintenance of operating procedures to ensure the secure operation of information processing facilities for the County. The existence of standard operating procedures reduces organizational dependence upon individual and institutional knowledge. The process of creating standard operating procedures requires detailed examination of process activities, the reason behind them and, in relevant cases, how the process could be improved.

System and Network Operations Management addresses the following areas:

- Implementation of formal change management control procedures
- Separation of development, testing, and operational computing environments
- Reduction in the risk of exposure when external contractors provide information processing facilities for County systems or services
- Proper management of capacity planning
- Reduction of the risk of system failure due to inadequate testing and validation
- Prevention and detection of malicious software
- Routine data backups and storage
- Preparation and testing of procedures and facilities for restoration of backup data
- Logging and reporting of all services, activity and faults
- Protection of connected services from unauthorized access and the security of data on networks
- Security of all County operational system documentation
- Creation of software exchange agreements
- Electronic data interchange involving various forms of commerce
- Establishment and use of email systems
- Internet Usage
- Use of publicly available methods of access (e.g., the Internet) to County information resources

6.2 POLICY STATEMENT

6.2.1 Operating procedures and responsibilities for all County information processing facilities should be formally authorized, documented, and maintained.

6.2.2 Changes to all information processing facilities, systems, software, or procedures should be strictly controlled according to formal change management procedures.

6.2.2.1 Unauthorized users should not make any changes to system and/or software configuration files.

6.2.2.2 Unauthorized users should not download and/or install operating system software, service-related software (such as web server software), or other software applications on County computer systems without prior written authorization from agency IT management. This includes, but is not limited to, free software, computer games and peer-to-peer file sharing software.

6.2.2.3 Each agency should develop a formal change control procedure that outlines the process to be used for identifying, classifying, approving, implementing, testing, and documenting changes to its IT resources.

6.2.2.4 Each agency should conduct periodic audits designed to determine if unauthorized software has been installed on any of its computers.

6.2.3 As appropriate, segregation of duties should be implemented by all County agencies to ensure that no single person has control of multiple critical systems and the potential for misusing that control.

6.2.4 Production computing environments should be separated from development and test computing environments to reduce the risk of one environment adversely affecting another.

6.2.5 System capacity requirements should be monitored and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.

6.2.6 System acceptance criteria for all new information systems and system upgrades must be defined, documented, and utilized to minimize risk of system failure.

6.2.7 Security awareness, prevention, and detection controls should be utilized to protect information systems and services against malicious software and against the unauthorized execution of mobile code (e.g., ActiveX controls, Java applets).

6.2.8 Backups of all essential electronically-maintained County business data should be routinely created and properly stored to ensure prompt restoration.

6.2.8.1 Each agency should implement and document a backup approach for ensuring the availability of critical application databases, system configuration files, and/or any other electronic information critical to maintaining normal business operations within the agency.

6.2.8.2 The frequency and extent of backups should be in accordance with the importance of the information and the acceptable risk as determined by each agency.

6.2.8.3 Agencies should ensure that locations where backup media are stored are safe, secure, and protected from environmental hazards. Access to backup media should be commensurate with the highest level of information stored and physical access controls should meet or exceed the physical access controls of the data's source systems.

6.2.8.4 Backup media should be labeled and handled in accordance with the highest sensitivity level of the information stored on the media.

6.2.8.5 Agencies should define and periodically test a formal procedure designed to verify the success of the backup process.

6.2.8.6 Restoration from backups should be tested initially once the process is in place and periodically afterwards. Confirmation of business functionality after restoration should also be tested in conjunction with the backup procedure test.

6.2.8.7 The system backup schedule should be published for users and is intended to ensure that users are aware of the procedures for the established backup process.

6.2.8.8 Agencies should retain backup information only as long as needed to carry out the purpose for which the data was collected, or for the minimum period required by law.

6.2.9 Systems operational staff should maintain appropriate log(s) of activities, exceptions and information security events involving County information systems and services.

6.2.10 Each agency should maintain a log of all faults involving County information systems and services.

6.2.11 Agencies should establish controls to ensure the security of the information systems networks that they operate.

6.2.12 When no longer required, the contents of removable media should be permanently destroyed or rendered unrecoverable in accordance with applicable agency, County, state, or federal record disposal and/or retention requirements.

6.2.13 Agencies should establish internal procedures for the secure handling and storage of all electronically-maintained County information that is owned or controlled by the agency.

6.2.14 Operational system documentation for County information systems should be protected from unauthorized access.

6.2.15 Agreements should be implemented for the exchange of information between the County and other entities.

6.2.16 County information accessed via electronic commerce should have security controls implemented based on the assessed risk.

6.2.17 Electronic mail should be governed for acceptable use and shall be open to inspection or review by management to comply with County, state and federal laws and regulations as well as any applicable agency policies. The use of email for conducting County business should be based on business management decisions regarding the appropriateness of the medium.

6.2.17.1 The email system and network are primarily for official business only.

6.2.17.2 County or agency authorization for an individual to use encryption or other measures to protect or "lock" email messages shall not constitute consent by the County or agency to maintain any such message as private.

6.2.17.3 Each user of a County email system shall have an individual email account that is uniquely linked to that user. General purpose email accounts, however, may be used for departmental interaction between the public and County employees (e.g., the general email account webmaster@ocgov.com is used to communicate with the general public).

6.2.17.4 Users should not use an internal County email account assigned to another individual to send or receive messages.

6.2.17.5 Use of Internet (external) email systems from County networks and/or desktop devices is prohibited unless there is a compelling business reason for such use.

6.2.17.6 Users shall not configure or use automated forwarding of County email messages to Internet (external) email systems unless specifically authorized to do so with written authorization by County management.

6.2.17.7 Confidential or restricted documents sent as attachments to email messages shall be treated as confidential or restricted documents. These same restrictions shall apply to confidential or restricted information embedded within an email message as message text.

6.2.17.8 If a business need exists to communicate confidential information within the County it may be done so by email with permission of management by sending the email only to those who have a need to know the information and by marking it "CONFIDENTIAL."

6.2.17.9 Using email to communicate confidential information should be the exception, not the rule. Memoranda and reports on paper, telephone calls, and face-to-face meetings should be used in specific contexts (e.g., the communication of personnel matters).

6.2.17.10 Special features designed to filter out malicious software contained in either email messages or email attachments should be implemented on all County email systems.

6.2.17.11 Users should not delete email messages whose subject matter has been identified as relevant to pending or anticipated litigation or other legal processes.

6.2.17.12 Agencies will provide their users with training on the appropriate use of both the Internet and County email systems and on the handling of email messages and attachments.

6.2.18 The Internet/Intranet access is primarily for official business only. County workforce members may access the Internet for limited personal business only during nonworking time and in strict compliance with the other terms of this policy. If there is any doubt about whether a contemplated activity is appropriate for County business purposes, employees may consult with their immediate supervisor to help decide if a use is appropriate.

6.2.18.1 In order to control Internet content that is seen by County workforce members, Agencies may use Web-filtering or content-control software.

6.2.18.2 In order to monitor, track and log Internet sites visited during normal work hours, Agencies may monitor, track, log and report on County workforce members Internet traffic.

6.2.19 Public access to County electronic information resources should provide desired services in accordance with safeguards designed to protect County resources.

6.2.20 The clocks of all relevant information processing systems should be synchronized with an agreed upon accurate time source such as an established Network Time Protocol (NTP) service.

6.2.21 County issued rules for use and maintenance of computers and other equipment include:

- Liquids or magnets are not to be kept on or near computers, as these can cause serious damage
- All original software assigned to County workforce members must be available when the system needs to be serviced in case the software needs to be reinstalled
- When a computer problem is discovered, all details about the problem should be recorded/communicated on the appropriate form and/or when called into Service Desk or discussed with IT staff.
- Equipment should be plugged into a surge protector at all times
- Any damage to equipment is to be reported to the appropriate authorities

The County may, on occasion, issue additional rules concerning the use and maintenance of computers and other equipment.

6.2.22 County Agencies are responsible for establishing internal processes to ensure vulnerability management. This includes the efficient application of vendor-supplied patches or other mitigations based on the following levels of criticality. The related applications should be tested pre and post patch deployment.

- Level 1 – Maintenance: Patches addressing non-security related issues are to be applied at agency/department discretion
- Level 2 – Required: Patches addressing theoretical security vulnerabilities are to be applied within two weeks of notification of patch availability
- Level 3 – Mandatory: Patches addressing security vulnerabilities for which an exploit exists are to be applied within one week of notification of patch availability
- Level 4 – Urgent: Patches addressing security vulnerabilities currently being exploited by Internet attacks are to be applied within 48 hours of notification of patch availability. Level 4 urgent patches shall to use the Incident Process and Management portion of this Policy. Notification of patch status is to be sent to CEO/IT.

6.2.23 Security vulnerability management policy applies to routers, switches, servers, desktops and laptops owned by the County, whether located on the County's internal network, another facility or in the offsite possession of a County employee, contractor, vendor or customer. This also applies to any contractor, vendor or customer owned equipment connected to the County network.

6.3 RELATED POLICY

- Section 9: Information Security Incident Management

7 ACCESS CONTROL

7.1 PURPOSE

Access Control is defined to ensure only authorized access to County information systems and resources with the overarching goal of protecting the confidentiality, integrity, and availability of all County resources. Information access and County computing processes should be controlled on the basis of County business and applicable security policies.

Access Control addresses the following areas:

- Allocation of user access rights
- Management of user access privileges
- Prevention of the assignment of unauthorized access privileges
- Establishment of a standard for password controls
- Reinforcement of the use of effective passwords
- Guidelines for access and use of networks and networked services
- Guidelines for the use of wireless network access technology
- Guidelines for activity timeout procedures for any networked session
- Appropriate system utilities access
- Establishment of valid logon connection schedules
- Disclosure of unauthorized activity through the use of monitoring activity and tracking logs
- Prevention of system security compromises during the use of mobile computing devices
- Guidelines on security issues involved in remote access

7.2 POLICY STATEMENT

7.2.1 GENERAL ACCESS

7.2.1.1 Agencies should establish a procedure that ensures only users with legitimate business needs to access County IT resources are provided with user accounts.

7.2.1.1.1 Access to County information systems and information systems will be based on each user's access privileges. Access controls must ensure that even legitimate users cannot access stored information unless they are authorized to do so.

7.2.1.1.2 The owner of each non-public County system, or their designee, provides written authorization for all internal and external user access.

7.2.1.1.3 All access to internal County computer systems shall be controlled by an authentication method involving a minimum of a user identifier (ID) and password combination that provides verification of the user's identity.

7.2.1.1.4 All County workforce members are to be assigned a unique user ID to access the network.

7.2.1.1.5 A user account should be explicitly assigned to a single, named individual. No group or shared computer accounts are permissible except when necessary and warranted due to legitimate business needs. Such need must be documented prior to account creation and accounts activated only when necessary.

7.2.1.1.6 User accounts should not be shared with others including, but not limited to, someone whose access has been denied or terminated. If the person using another person's account violates this policy by using that account, it is considered to be the same as the original account owner violating policy. Both persons are then subject to the consequences of that violation.

7.2.1.1.7 By accepting account passwords and other information from the County and accessing the network or the Internet, County workforce members are agreeing to follow the IT Security policy.

7.2.1.1.8 County approved password standards and/or guidelines should be applied to the access of all County systems.

7.2.1.1.9 Passwords are a primary means to control access to systems and should therefore be selected, used, and managed to protect against unauthorized discovery or usage. (e.g., use passwords of eight or more characters, including at least one number and one uppercase character).

7.2.1.1.10 Passwo rd management systems should be deployed where feasible to comply with the County Single Sign-On Initiative.

7.2.1.1.11 Periodic log reviews of user access and privileges should be performed in order to monitor access of sensitive information.

7.2.1.1.12 Auditing and logging of user activity should be implemented on all critical County systems that support user access capabilities.

7.2.1.1.13 All workforce members are responsible for creating and maintaining the confidentiality of the password associated with their unique user ID. Upon receipt of a user ID, the person assigned the user ID is required to change the temporary password provided by the administrator to a password known only to the user.

7.2.1.1.14 Ne wly-created accounts should be assigned a randomly-generated password prior to account information being provided to the user.

7.2.1.1.15 No user shall give his or her password to another person under any circumstances. Workforce members who suspect that their password has become known by another person shall change their password immediately and report their suspicion to management in accordance with Section 9: Incident Management.

7.2.1.1.16 Users who have lost or forgotten their passwords must make any password reset requests themselves without using a proxy (e.g., another County employee) unless approved by management. Prior to processing password change requests, the requester must be authenticated to the user account in question. (e.g. Verification with user's supervisor or the use of passphrases can be used for this authentication process.) New passwords should be provided directly and only to the user in question.

7.2.1.1.17 Agenci es should require workforce members to change their network and application passwords periodically (e.g., every 90 days at the maximum). Changing passwords more often than 90 days is encouraged.

7.2.1.1.18 Whe n technologically feasible, network and application systems should be configured to enforce automatic expiration of passwords at regular intervals (e.g., every 90 days at the maximum).

7.2.1.1.19 When technologically feasible, a new or reset password shall be set to expire on its initial use at log on so that the user is required to change the provided password to one known only to them.

7.2.1.1.20 All privileged system-level passwords (e.g., root, enable, OS admin, application administration accounts, etc.) should be changed at least every 90 days.

7.2.1.1.21 All passwords are to be treated as sensitive and highly confidential information.

7.2.1.1.22 At the time of network login, the user shall be presented with a County Council-approved statement ("login banner") containing language regarding the appropriate use of computer systems.

7.2.1.1.23 Employees may be asked from time-to-time to provide new or additional registration and account information, for example, to reflect developments in the law or technology. Employees must provide this information if they wish to continue to receive service. If after employees have provided their account information, some or all of the information changes, employees must notify the person designated by the County to receive this information.

7.2.1.2 Automated screen lockouts should be used wherever possible using a set time increment (e.g., 15 minutes of non-activity). In situations where it is not possible to automate a lockout, operational procedures should be implemented to instruct users to lock the terminal or equipment so that unauthorized individuals cannot make use of the system. Once logged on, workforce members should normally not leave their computer unattended or available for someone else to use.

7.2.1.3 Access to a the County network and its resources should be strictly controlled, managed, and reviewed to ensure only authorized users gain access based on the privileges granted. (e.g., Kiosks provide physical and public access to County networks. These should be secured to ensure County resources are not accessed by unauthorized users.)

7.2.1.4 The control mechanisms for all types of access to County IT resources by contractors, customers or vendors are to be documented.

7.2.1.5 System utilities should be available to only those users who have a business case for accessing the specific utility.

7.2.1.6 All applications are to have access controls unless specifically designated as a public access resource.

7.2.1.7 When deemed necessary, user logins and data communications may be restricted by time and date configurations that limit when connections will be accepted.

7.2.1.8 The decision to use cryptographic controls and/or data encryption on a hard drive should be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.

7.2.2 COUNTY WIRELESS ACCESS

7.2.2.1 Agencies shall take appropriate steps, including the implementation of appropriate encryption, user authentication, device authentication and malware protection measures, to mitigate risks to the security of County data and information systems associated with the use of wireless network access technologies.

7.2.2.1.1 Only wireless systems that have been evaluated for security by both agency management and by the CIO should be approved for connectivity to County networks.

7.2.2.1.2 County data that is transmitted over any wireless network must be protected.

7.2.3 NON-COUNTY ACCESS

7.2.3.1 All access to County networks or resources via unapproved wireless communication technologies is prohibited. This includes wireless systems that may be brought into County facilities by visitors or guests. Employees, contractors, vendors and customers are prohibited from connecting and/or activating wireless connections on any computing device that are simultaneously connected to any County network, either locally or remotely.

7.2.3.2 Each agency should make a regular, routine effort to ensure that unauthorized wireless networks, access points, and/or modems are not installed or configured within its IT environments. Any unauthorized connections described above should be disabled immediately.

7.2.3.3 All remote access implementations that involve non-County infrastructures should be reviewed and approved by both the agency ISO and the CIO or their designee. This approval should be received prior to the start of such implementation. The approval should be developed as a memorandum of understanding (MOU).

7.2.3.4 Any computing device, including laptops and desktop PCs, that has been connected to a non-County infrastructure (including employee home networks) and subsequently used to connect to the County network should be verified that it is free from viruses and other forms of malicious software prior to attaining connectivity to the County network.

7.2.3.5 Remote access privileges to County IT resources should not be given to contractors, customers or vendors unless agency management determines that these individuals or organizations have a legitimate business need for such access. If such access is granted, it should be limited to those privileges and conditions required for the performance of the specified work.

7.2.4 REMOTE ACCESS

7.2.4.1 Agencies shall take appropriate steps, including the implementation of appropriate encryption, user authentication, and virus protection measures, to mitigate security risks associated with allowing users to use remote access or mobile computing methods to access County information systems.

7.2.4.1.1 Remote access privileges should be granted to County workforce members only for legitimate business needs and with the specific approval of agency management.

7.2.4.1.2 All remote access implementations that utilize the County's trusted network environment and that have not been previously deployed within the County should be submitted to and reviewed by the CIO's office. A memorandum of understanding (MOU) should be utilized for this submittal and review process.

7.2.4.1.3 Session inactivity timeouts should be implemented for all remote access into and from County networks.

7.2.4.1.4 All remote access infrastructures must include the capability to monitor and record a detailed audit trail of each remote access attempt.

7.2.4.1.5 All users of County networks and computer systems are prohibited from connecting and/or activating unauthorized dial-up or broadband modems on workstations, laptops, or other computing devices that are simultaneously connected to any County network.

7.2.4.1.6 Each agency will conduct regular internal audits in order to identify unauthorized remote connections.

7.2.4.1.7 Users granted remote access to County IT infrastructure must follow all additional policies, guidelines and standards related to authentication and authorization as if they were connected locally. For example, this applies when mapping to shared network drives.

7.2.4.1.8 Users attempting to use external remote access must utilize a County-approved multi-factor authentication process.

8 SYSTEMS DEVELOPMENT AND MAINTENANCE

8.1 PURPOSE

The integration of security measures with systems development, customization, and maintenance activities ensures that business applications, mission-critical software and commercial off-the-shelf software (COTS) do not become a security threat to the organization's assets. County applications, mission-critical software and COTS should be implemented and maintained in a safe and effective manner. If there is a conflict between Federal and State owned or controlled systems and this policy, the Federal and State owned or controlled systems prevail over this policy.

System Development and Maintenance addresses:

- Security related business requirements for new systems or enhancements to existing systems
- Controls for integration into applications to ensure that each level or type of information access is secure at a consistent level
- Controls on data input, output, access and processing
- Cryptographic security controls for new systems or enhancements to existing systems
- Securing operating system files and application software
- Securing system test data
- Securing access to program source libraries
- Change controls for systems development and maintenance
- Change or upgrade processes for production operating systems
- Purchased software and changes to executable code provided by a vendor
- Avoiding unauthorized introduction of unintentional and intentional malicious software

8.2 POLICY STATEMENT

8.2.1 GENERAL

8.2.1.1 Agencies should identify all business applications that are used by their users in support of primary business functions. This includes all applications owned and/or managed by the agency as well as other business applications that are used by the agency but owned and/or managed by other County organizations. All business applications used by an agency should be documented in the agency's IT security plan as well as their Business Impact Analysis (BIA).

8.2.1.2 An application owner should be designated for each internal agency business application.

8.2.1.3 All access controls associated with business applications should be commensurate with the highest level of data used within the application. These same access controls should also adhere to the policy provided in Section 7: Access Control.

8.2.1.4 Security requirements should be incorporated into the evaluation process for all commercial software products that are intended to be used as the basis for a business application. The security requirements in question should be based on requirements and standards specified in this policy

8.2.1.5 In situations where data needs to be isolated because there would be a conflict of interest (e.g., DA and OCPD data cannot be shared), data security will be designed and implemented to ensure that isolation.

8.2.2 REQUIREMENTS

8.2.2.1 The business requirements definition phase of system development must contain a review to ensure that the system will adhere to County information security standards.

8.2.3 CORRECT PROCESSING OF APPLICATIONS

8.2.3.1 Owners of IT systems should implement checks on data input to ensure the data is correct and appropriate. An example of this is utilizing input checks to detect: out-of-range values, invalid characters, missing or incomplete data, and data exceeding upper or lower volume limits or unauthorized or inconsistent control data.

8.2.3.2 Owners of IT systems should use validation checks within applications to detect any corruption of information through processing errors or deliberate acts. An example of this is the use of appropriate programs to recover from a failure to ensure the correct processing of data.

8.2.3.3 Owners of IT systems should ensure the authentication of all messages sent and received within those systems. An example of this is using cryptographic techniques to authenticate messages containing confidential or sensitive information.

8.2.3.4 Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the business transaction. An example of this is using reconciliation control counts to ensure processing of all data.

8.2.4 CRYPTOGRPAHIC CONTROLS

8.2.4.1 The decision to use cryptographic controls and/or data encryption in an application should be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.

8.2.4.1.1 Where appropriate, encryption should be used to protect confidential or restricted application data that is transmitted over open, untrusted networks, such as the Internet.

8.2.4.1.2 When cryptographic controls are used, procedures addressing the following areas should be established by each agency:

- Determination of the level of cryptographic controls
- Key management/distribution steps and responsibilities

8.2.4.1.3 Encryption keys should be exchanged only using secure methods of communication.

8.2.4.1.4 To ensure interoperability, encryption technologies should be based on the architecture standards established by the CIO.

8.2.5 SYSTEM FILES

8.2.5.1 Operating system files, application software and data should be secured from unauthorized use or access.

8.2.5.2 Clear-text data that results from testing should be handled, stored, and disposed of in the same manner and using the same procedures as are used for production data.

8.2.5.2.1 System tests should be performed on data that is constructed specifically for that purpose.

8.2.5.2.2 System testing should not be performed on operational data unless the necessary safeguards are in place.

8.2.5.3 A combination of technical, procedural and physical safeguards should be used to protect application source code from unintentional or unauthorized modification or destruction. All County proprietary information, including source code, needs to be protected through appropriate role-based access controls. An example of this is a change control tool that records all changes to source code including new development, updates, and deletions, along with check-in and check-out information.

8.2.6 SYSTEM DEVELOPMENT & MAINTENANCE

8.2.6.1 Policies established by this IT Security Policy will be incorporated into the system development of new business applications that are developed internally or that are developed for County or agency use by vendors, contractors or consultants.

8.2.6.2 The development of software for use on County information systems must have documented change control procedures in place to ensure proper versioning and implementation.

8.2.6.3 When preparing to upgrade any County information systems, including an operating system, on a production computing resource; the process of testing and approving the upgrade should be completed in advance in order to minimize potential security risks and disruptions to the production environment.

8.2.6.4 Systems should be hardened and logs monitored to ensure the avoidance of the introduction and exploitation of malicious code.

8.2.6.4.1 All County workforce members shall not create, execute, forward, or introduce computer code designed to self-replicate, damage, or impede the performance of a computer's memory, storage, operating system, or application software.

8.2.6.5 In conjunction with other access control policies, any opportunity for information leakage should be prevented through good system design practices.

8.2.6.6 Agenci es are responsible for monitoring outsourced software development related to agency-owned IT systems.

8.3 RELATED POLICY

- Section 7: Access Control.
- Sections 6.2.2 – 6.2.2.4: Change Control information

9 INFORMATION SECURITY INCIDENT MANAGEMENT

9.1 PURPOSE

Information Security Incident Management establishes the policy to be used by each agency in planning for, reporting on, and responding to computer security incidents. For these purposes an incident is defined as any irregular or adverse event that occurs on a County system or network.

9.2 POLICY STATEMENT

9.2.1 Security incident management procedures should be established within each agency to ensure quick, orderly, and effective responses to security incidents.

The steps involved in managing a security incident are typically categorized into six stages:

- System preparation
- Problem identification
- Problem containment
- Problem eradication
- Incident recovery
- Lesso ns learned

9.2.1.1 Agencies should document procedures for reporting security incidents through appropriate management channels.

9.2.1.2 Agencies should document procedures for intrusion detection.

9.2.2 Agencies should establish procedures to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

9.2.3 Where a follow-up action against an entity after an information security incident will involve civil or criminal legal action, evidence should be collected, retained, and presented to conform to the rules for evidence as demanded by the relevant jurisdiction(s). At the Agency's discretion, they may obtain the services of qualified external professionals to complete these tasks.

9.2.4 Each agency should designate one individual as its Information Security Officer (ISO). The ISO will act as the liaison between applicable parties during a security incident. The ISO will be a member of the Information Security Team (IST) as well as the agency's primary point of contact for all IT security issues. The agency ISO should designate an alternate contact to act as the liaison should s/he be unavailable.

9.2.4.1 A directory or phone tree should be created listing all agency security incident liaison contact information.

9.2.4.2 Each agency shall train its employees on the use of its security incident reporting procedures.

9.2.5 Each agency shall develop a procedure for users to report perceived threats to the security of information systems. For example, all employees, contractors, vendors and customers of County information systems should be required to note and report any observed or suspected security weaknesses in systems to management. In the event an agency has not established these procedures, the County ISO may be contacted for assistance.

9.2.6 Agencies will respond to security advisory information received from either internal (e.g., County) or approved external sources by promptly undertaking appropriate and/or recommended procedures intended to mitigate the effects of actual or potential security incidents.

9.2.7 Contact with local authorities, including law enforcement, shall be conducted through an organized, repeatable process that is both well documented and communicated.

9.2.8 Contact with special interest groups, including media and labor relations, shall be conducted through an organized, repeatable process that is both well documented and communicated.

10 BUSINESS CONTINUITY AND DISASTER RECOVERY

10.1 PURPOSE

Business Continuity is intended to counteract interruptions in business activities and to protect critical business processes from the effects of significant disruptions. Disaster Recovery provides for the restoration of critical County assets, including IT infrastructure and systems, staff, and facilities.

10.2 POLICY STATEMENT

10.2.1 Each agency shall develop, periodically update, and regularly test business continuity and disaster recovery plans in accordance with the County's Business Continuity Management Policy.

10.2.2 Agencies will, at a minimum, review and update their Risk Assessments (RAs) and Business Impact Analyses (BIAs) on an annual basis. As detailed in Section 12: Risk Assessment and Treatment, RAs include agency identification of risks that can cause interruptions to business processes along with the probability and impact of such interruptions and the consequences to information security. A BIA establishes the list of processes and systems that the agency has deemed critical after performing a risk analysis.

10.2.3 Continuity plans should be developed and implemented to provide for continuity of business operations in the event that critical IT assets become unavailable. Plans must provide for the availability of information at the required level and within the established Recovery Time Objective (RTO)

10.2.4 Each agency should maintain a comprehensive plan document containing its business continuity plans. Plans should be consistent, address information security requirements, and identify priorities for testing and maintenance. Plans should be prepared in accordance with the standards established by the County's Business Continuity Management Policy.

10.3 RELATED POLICY

- County Business Continuity Management Policy
- Section 12: Risk Assessment and Treatment

11 COMPLIANCE

11.1 PURPOSE

Compliance establishes the operation of County information systems in accordance with applicable law; statutory, regulatory or contractual obligations; and security requirements.

11.2 POLICY STATEMENT

11.2.1 The County Information Security Policy must comply with state and federal regulations all well as identify the relevant statutory and regulatory requirements.

11.2.2 Each agency should implement appropriate procedures to ensure compliance with state and federal regulations on the use of intellectual property.

11.2.3 Each agency should acquire software only through known and reputable sources to ensure that software licensing and copyrights are not violated.

11.2.4 Agency management should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

11.2.5 Agencies should periodically review written procedures and information systems to ensure ongoing compliance with security policies and applicable standards.

11.2.6 Agencies should develop formal IT audit policy and procedures. Audit policy and procedures should address the following:

- The type of processes to be audited
- Use of read-only access to data to conduct the audit
- Planning for audits on operational systems to minimize the risk of disruptions to business processes.
- Avoiding conflicts of interest by putting in place an independent auditor (i.e., someone who does not participate in the activities being audited)
- Protection of information systems audit tools to prevent any possible misuse or compromise.

11.2.7 The use of the network and Internet is a privilege, not a right. If policy is violated, the offender may be subject to termination of network and/or Internet access. The County may refuse to reinstate such access for the remainder of the offender's tenure at the County. The County may also take other disciplinary action as allowed under County policy. A violation of this policy may also be a violation of the law and subject the user to investigation and criminal or civil prosecution.

11.3 RELATED POLICY

11.3.1 Section 2: Information Technology Security

12 RISK ASSESSMENT AND MITIGATION

12.1 PURPOSE

Risk assessments should identify, quantify, and prioritize risks against County assets, systems, processes and deliverables. The results should guide and determine the priorities for information security risk management and for implementing controls selected to protect against risks. Mitigation of risks furthers the County's goal of protecting its assets from harm.

12.2 POLICY STATEMENT

12.2.1 Agencies should develop and implement risk assessment policies based on Best Practices that should include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).

12.2.2 Agencies should perform the process of assessing risks and selecting the controls for coverage of multiple organizational information assets or individual information systems.

12.2.3 Risk assessments should be performed periodically to address changes in the security requirements and in the risk situation, e.g., changes in assets, threats, vulnerabilities, impacts, or risk evaluation methodologies and when significant infrastructure changes occur. These risk assessments should be undertaken in a methodical manner capable of producing reproducible results.

12.2.4 Before considering risk mitigation, the agency should decide criteria for determining whether or not risks can be accepted. Risks may be accepted if, for example, it is assessed that the risk is low or that the cost of mitigation is not cost-effective for the agency.

12.2.5 For each of the risks identified following the risk assessment, a risk mitigation decision needs to be made. Possible options for risk mitigation include:

- Risk Limitation - applying appropriate controls to reduce the risks
- Risk Assumption - knowingly and objectively accepting risks, providing such acceptance satisfies the organization's policy and criteria for risk acceptance
- Risk Avoidance - avoiding risks by not allowing actions that would cause the risks to occur
- Risk Transference - transferring the associated risks to other parties, e.g., insurers or suppliers

12.2.6 For those risks where the risk mitigation decision has been to apply appropriate controls, these controls should be selected and implemented to meet the requirements identified by the risk assessment. Controls should ensure that risks are reduced to an acceptable level, taking into account:

- Requirements and constraints of County, state and federal legislation and regulations
- Orga nizational objectives
- Operational requirements and constraints

- Cost of implementation and operation in relation to the risks being reduced and keeping mitigation costs proportional to the organization's requirements and constraints
- Need to balance the investment in implementation and operation of controls against the harm likely to result from security failures

12.3 RELATED POLICY

- Business Continuity Management Policy

13 PRIVACY

13.1 PURPOSE

Personal Identifiable Information (PII) should be protected from unauthorized use. The unauthorized use of PII is the leading cause of identity theft; specifically national identification numbers or Social Security Numbers.

13.2 POLICY STATEMENT

13.2.1 All County workforce members with access to PII shall treat information as confidential and take all secure precautions necessary to ensure this information is not compromised. The accidental or intentional disclosure of PII to unauthorized users is in violation of this policy.

13.2.2 All information created, sent, or received via the email system, network, Internet, telephones or the Intranet is the property of the County. Employees should not have any expectation of privacy regarding such information. This includes all email messages and electronic files. The County reserves the right to, at any time and without notice, access, read and review, monitor, and copy all messages and files on its computer system as it deems necessary. When it believes necessary, the County may disclose text or images to law enforcement without the employee's consent.

13.2.3 All hardcopy or printed materials containing PII shall be treated as confidential information. This should not be left unattended for any period of time. This information should be physically destroyed by an approved process before discarding it.

14 APPENDIX A: DEFINITIONS

The following definitions apply to all policies presented in this document, as well as to all other documents developed as part of the County's IT Security efforts.

*For purposes of this document, the following three terms are to be interpreted as the definitions indicate.

Must: This word, or the term "SHALL", mean that the policy is an obligation.

Shall: must; is or are obliged to

Should: This word means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

ALPHABETICAL LISTING (A – Z)

Agency/Department: Any reference to "agency" or "department" refers to County agencies, departments, and/or County managed organizations that operate within the trusted environment.

Application Owner: A designated individual within an agency who is responsible for defining and enforcing the application's operating parameters, authorized functions, and security requirements.

Authentication: Process during which valid users are uniquely identified, and their identification is verified, prior to being given access to County information assets.

Authorization: Following authentication, the level of privileges that are assigned to individual users of IT resources.

Authorized: To have been granted officially sanctioned and accurate access to an IT resource.

Backup: The process of copying/duplicating files, databases, and/or system files to avoid loss of data and to facilitate recovery in the event of a system problem or failure.

Business Continuity: The ability of an organization to provide service and support for its customers and to maintain its viability before, during, and after a business disruption.

Business Continuity Plan: Management approved document that defines the arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period of time and to return to performing its critical business functions after an interruption.

CERT: Computer Emergency Response Team

Change Control: A combination of technical, physical, and procedural safeguards used to protect systems and/or software applications from unintentional and/or unauthorized modification.

CIO: Chief Information Officer for the County

Clear-text data: data stored or transferred without cryptographic protection

Compliance: Conformation to local, state, and federal laws and to the IT Security Policy set forth by the County.

Confidentiality/Non-Disclosure Agreement: An agreement between at least two parties that outlines confidential materials or knowledge the parties wish to share with one another for certain purposes, but wish to restrict from generalized use. The parties agree not to disclose information covered by the agreement.

Contractor: A temporary non-employee conducting authorized business within County resources via access rights similar to those of County employees. For these purposes, "consultant" is synonymous with "contractor".

County (of Orange): For the purposes of this document, any reference to "County" is to be interpreted as "County of Orange".

County ISO: The County Executive Office Information Security Officer.

County Workforce Members: All employees, contractors, vendors and customers working to forward the County's mission.

Cryptographic Controls: Controls used to secure County information resources, such as data encryption, digital signatures, non-repudiation services, and key management.

Customer: Anyone who receives services from the County.

DAD: Director of Application Development.

Data/Information: Any communication or information, including but not limited to numeric, graphic, or narrative information, maintained on any medium including, but not limited to, computerized databases, paper, microform, optical/magnetic disk, magnetic tape, and/or in transit over a communications network. No distinction is made between the word "data" and "information" for purposes of the IT Security Policy.

Development Oversight: Review of software and application development for security risks. This includes Software Quality Assurance (SQA) techniques.

Disaster: A sudden, unplanned catastrophic event causing unacceptable damage or loss. (1) An event that compromises an organization's ability to provide critical functions, processes, or services for some unacceptable period of time. (2) An event where an organization's management invokes its recovery plans.

Disaster Recovery: The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.

Disaster Recovery Plan: Management approved document that defines the processes, resources, actions, tasks and data required to manage technology and infrastructure recovery efforts. This is a component of the Business Continuity Management Program.

DSO: Director of Systems Operations.

Encryption: The process of transforming information (referred to as "plaintext") using an algorithm (a "cipher") to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

> *Algorithm (Encryption):* A set of ordered steps for solving a problem, such as a mathematical formula or the instructions in a program. This is used in conjunction with a key to encrypt or decrypt information.

Data (Encryption): The process and result of using encryption on electronic information (data) to secure it from unauthorized access.

Data at Rest (Encryption): Encryption of data that is located in a single location, such as a hard drive or tape storage.

Data in Transit (Encryption): Encryption of data that is transmitted from point A to point B. Data in transit encryption can be performed via email; XML at the application layer; or in network packets at the data link, network or transport layers.

Key: A secret numeric code that is used to encrypt text for security purposes.

Key Management (Encryption): The secure creation, management, storage and use of encryption keys.

Key Distribution (Encryption): The secure distribution and exchange of encryption keys between parties using encrypted communication. This includes how keys are made available to both parties. For example, using asymmetric encryption requires the use of public keys that could be stored on a public directory website.

Enterprise: The entire County and its attendant entities, including all agencies and departments that operate within the trusted environment. The enterprise excludes special districts such as OCTA, Law Library, and the Cemetery District.

Environmental Threat: Any threat to County operations that is manifested via the environment including, but not limited to, fire, flood/water damage, earthquake, severe weather, and airborne toxins.

External Threat: Any threat to County operations that is manifested from outside the County enterprise.

Guidelines: A guideline is similar to a standard or policy in that it outlines a specific principle, direction, directive, specification, or procedure. Unlike a standard or policy, a guideline is not binding but is instead a recommended course of action.

IID (Internal Intrusion Detection): Detection of an intrusion generated by misuse or attempted misuse of organizational resources by legitimate users.

Incident: The term incident in this document is defined as any irregular or adverse event that occurs on a County system or network. Examples of incidents include:

- Loss of service, equipment or facilities
- System malfunctions or overloads
- Huma n errors
- Non-compliances with policies
- Breaches of physical security
- Unplanned or unauthorized system changes
- Malfunctions of software or hardware
- Acce ss violations

Incident Response: The process of formally acting and reporting on an incident that has been identified to the Incident Management Team, the Information Security Officer, or appropriate management.

Information Classification: The labeling of information assets according to their sensitivity to disclosure. Label include *Confidential, Sensitive, Restricted* and *Public.*

Information Processing Facilities: A physical or logical entity that is used in the processing of information within the scope of the County. Examples include a complete data center, a new database application or a single laptop.

Information Security Infrastructure: The complete set of information security-related systems, procedures, policies and physical implementations of information security administration.

Information Security Management: Management of all agency-related information security issues including: (1) Formulation, review and approval of agency information security policy; (2) Maintenance of threat assessments for internal information; (3) Oversight of investigations into security-related incidents; and (4) Oversight of business issues regarding new security initiatives.

Information Security Team: The Information Security Team (IST) is an Agency-defined team that will act as the incident coordination team for all Agency-related security incidents. An example of a team framework includes the SA, DSO, DAD, and Departmental CIO.

Information Systems: Any combination of computer hardware and software that generates, processes, transmits, accepts, and/or stores data or information.

Information Systems Application / Business Application: Any software program that has been developed, acquired, or modified specifically to support a unique and identifiable County business function. This includes applications used across multiple agencies and/or departments.

IT Security Policy: A general or high level statement of a direction, purpose, and principle for managing and protecting technology and technology resources.

Local Security Administrator: Resource identified within each agency that is responsible for the operational maintenance of IT security resources within the agency.

Loss of Data: The unforeseen loss of data or information.

Misuse: Any use of information, systems and resources that is out of compliance or is in conflict with County policies, applicable state and federal laws and/or County IT Security Policy.

Mobile Computing: Any computing device that can be disconnected from one network and re-attached to another network. This includes portable devices such as notebook computers, Personal Digital Assistants (PDAs), smart phones, pocket PCs and Lo-jack or other real-time tracking devices. This also includes desktop PCs in those circumstances where the desktop device is disconnected from one network and then reconnected to another network. Since wireless access devices work in this manner, they are also considered to be mobile computers for the purposes of this policy.

Non-County Infrastructure: Any network or environment in which the device(s) and/or network equipment are not under the direct control and management of designated County IT network support staff. This includes, but is not limited to, vendor facilities, other government facilities, employee homes, the Internet, and devices in County facilities that are not directly connected to the County's network.

NTP (Network Time Protocol): A mechanism for synchronizing the clocks of computer systems over packet-switched data networks.

Offender: Someone who violates County policy or any local, state, or federal law or regulation.

Operational System Documentation: Operational manuals, tables, access control lists, or other documentation that contain sensitive information which, if divulged, could compromise the security of the systems referenced within such documentation. (e.g., network diagrams, router configurations, firewall rule sets, etc.)

Personal Identifiable Information (PII): any piece of information that can potentially be used to uniquely identify, contact, or locate a single person. Examples include full name, national identification number, driver's license number, etc.

Personnel Screening/Background Check: Use of a defined, repeatable process to verify a person's background. An example includes a system such as LiveScan.

Physical Threat: Any threat to County operations that is manifested physically. Examples include civil unrest, physical sabotage, and physical assault of facilities.

Procedures: Specific steps, tasks, and activities to be performed to implement IT security policy. As a general rule, agencies and/or departments are responsible for establishing procedures that adhere to the County IT Security Policy.

Remote Access: Any access of County IT assets from a non-County infrastructure (including employee homes), no matter what technology is used to gain access.

Risk Assessment: The process by which risks are identified and the impact of those risks determined.

SA: Security Administrator.

Security Awareness/Training: The process of educating all County users about the IT Security Policy and/or all appropriate agency Information Security Policies.

Security Plan: In the context of the County IT Strategic Plan and this document, the security plan includes security policy, procedures and standards. The County is developing a security plan including this security policy with procedures/standards to follow. Agencies will also develop security plans including an Agency security policy, procedures and standards.

Security Working Group: A committee assembled from security resources throughout the County. Its primary function is to discuss security issues and technologies and to create security policies and guidelines for use by all County agencies and departments.

Standards: A prescribed or proscribed specification, approach, directive, procedure, solution, methodology, product or protocol that must be followed in order to comply with the IT Security Policy.

Systems Development: The process by which an information systems application is created and deployed. This general term is used to describe the entire lifecycle of a new County application, including requirements gathering, coding, testing, implementation and deployment, and retirement.

System Hardening: The process of eliminating or minimizing vulnerabilities on a computer system. Techniques used include anti-virus software; firewalls; configuration changes to remove unused access points (e.g., email, web and FTP servers/ports); and patch level maintenance.

Systems Maintenance: The process of updating existing County information system applications, including application and/or operating system code and configuration changes.

Theft: The illegal taking of another's property without that person's freely given consent.

Trusted Environment: An information system and network or combination of systems/networks that is under the direct control and management of County personnel.

Written Authorization: Methods include email, memo, letter, security access change form, and change in active directory or user account database.

Users: Any reference to "users" should be interpreted as individuals accessing and/or using County IT assets, including full or part-time employees, contractors, consultants, interns, volunteers, and any other authorized individuals attempting access or use of the County's IT infrastructure.

Vault: A double-locking manhole cover that prevents unauthorized access from the street level.

Vendor: Any entity that sells or provides services to the County.

15 APPENDIX B: IT ETIQUETTE

All users must abide by rules of network etiquette, which include being polite and using the network and the Internet in a safe and legal manner.

16 APPENDIX C: PROHIBITED ACTIVITY

The County or authorized County officials will make a good faith judgment as to which materials, files, information, software, communications, and other content and activities are permitted and prohibited based on the following guidelines and under particular circumstances.

Unless workforce members are specifically authorized due to their work assignment, the following are among uses that are considered unacceptable and constitute a violation of this policy:

(a) Using, transmitting, or seeking inappropriate or offensive materials, including vulgar, profane, suggestive, obscene, abusive, harassing, belligerent, threatening, or defamatory (harming another's reputation by lies) language or materials.

(b) Revealing PII without permission, such as another's home address, telephone number, credit card number or Social Security Number.

(c) Making offensive or harassing statements or jokes about language, race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.

(d) Sending or soliciting sexually oriented messages or images.

(e) Visiting sites featuring pornography, terrorism, espionage, theft, drugs or other subjects that violate or encourage violation of the law.

(f) Gambling or engaging in any other activity in violation of local, state, or federal law.

(g) Uses or activities that violate the law or County policy or encourage others to violate the law or County policy. These include:

- Without proper authorization, accessing, transmitting, or seeking confidential information about clients or coworkers
- Conducting unauthorized business
- Intruding, or trying to intrude, into the folders, files, work, networks, or computers of others, or intercepting communications intended for others
- Knowingly downloading or transmitting confidential information

(h) Uses that cause harm to others or damage to their property. These includes:

- Downloading or transmitting copyrighted materials without the permission of the copyright owner. Even if materials on the network or the Internet are not marked with the copyright symbol, ©, one should assume that they are protected under copyright laws unless there is explicit permission stated concerning their use
- Using another's password or other user identifier that misleads message recipients into believing that someone other than the authenticated user is communicating or otherwise using the other's access to the network or the Internet
- Intentionally uploading a virus, other harmful component, or corrupted data or vandalizing any part of the network
- Using any software on the network other than that licensed or approved by the County.

(i) Uses that jeopardize the security of and access to the County network or other networks on the Internet

(j) Accessing, attempting to access, or encouraging others to access controversial or offensive materials. Be advised that access to the network and the Internet may include the potential for access to materials inappropriate for use in County business, including materials that may be illegal, defamatory, or offensive. Certain of these areas on the Internet may contain warnings as to their content and users are advised to heed these warnings. Not all sites that may contain inappropriate material, however, will include warnings. Responsibility must be taken for use of the network and the Internet and these sites must be avoided.

(k) Commercial uses. Do not:

- Buy or sell anything over the Internet
- Solicit or advertise the sale of any goods or services (whether to one recipient or many, such as "junk e-mail")
- Use County information technology for unauthorized outside fund-raising activities, participating in any lobbying activity, or engaging in any prohibited partisan political activity
- Use County information technology to post County, department and/or other public agency information to external news agencies, service bureaus, bulletin boards or other forums except with prior authorization

(l) Uses that waste limited resources. For example:

- Printing of personal files, which wastes toner or paper in printers.
- Chain letters, even for noncommercial or apparently "harmless" purposes, as these, like email with large graphic attachments and "junk e-mail," use limited network resources.
- Including unnecessary recipients on an email. Only copy others on an email who should be "in the loop" on the topic addressed.
- Indiscriminate use of distribution lists. Before using a distribution list, determine whether or not it is appropriate for everyone on that list to receive the email.
- "All hands" emails. Emails of this type are to be sent only after management permission has been obtained.

17 APPENDIX D: RESPONSIBILITIES

17.1 INFORMATION TECHNOLOGY SECURITY

17.1.1 Agency management has the ultimate responsibility for ensuring that all individuals within their organizations understand and comply with the IT Security Policy.

17.1.2 All users with either direct or indirect access to County information systems are responsible for understanding and complying with the IT Security Policy as well as any additional policies or procedures mandated by the individual agencies.

17.2 ORGANIZATIONAL SECURITY

17.2.1 The County is responsible for providing a basic security infrastructure framework to be used by all agencies and/or departments within the County. Where agency business need exceeds the County-provided security infrastructure, the agency is responsible for working collaboratively with CEO/IT to determine and implement a solution.

17.2.2 All persons that engage the services of or work with contractors, vendors or customers are responsible for understanding and adhering to organizational security policy.

17.3 HUMAN RESOURCES SECURITY

17.3.1 Agency management is responsible for following this policy and for ensuring their employees follow this policy.

17.3.2 Agency management is responsible for conducting disciplinary procedures as appropriate.

17.3.3 Agency management is responsible for initiating changes to access rights. The local security administrators are responsible for processing these requests and confirming their completion with the requesting manager or supervisor.

17.3.4 A County workforce member's responsibility for information security should be reviewed annually.

17.4 PHYSICAL AND ENVIRONMENTAL SECURITY

17.4.1 All County agencies that house information processing facilities are responsible for implementing procedures to follow the physical and environmental security policy, including identifying the perimeter of the facility and performing a risk analysis to assess its physical security.

17.4.2 All County employees, contractors, vendors and customers are required to adhere to the physical and environmental security policies established by the authorized agency.

17.5 SYSTEM AND NETWORK OPERATIONS MANAGEMENT

17.5.1 The Local Security Administrator, in conjunction with the agency director and the agency ISO, is responsible for implementing procedures to follow the operations and communications security policy listed in this document.

17.5.2 Each system administrator is responsible for providing a quarterly report to agency management listing all unaccessed user accounts. Upon the completed review of this report, system administrators are to take appropriate action as directed by agency management.

17.5.3 All County employees, contractors, vendors and customers that work in an operational and communication role are required to adhere to the operations and communications security procedures established by the related agency.

17.5.4 CEO/IT is responsible for the assignment of patch criticality levels. Criticality levels will be assigned based upon notification from DHS, InfraGard, SANS or Security Focus. CEO/IT is further responsible for the publication of patch availability notifications as well as for policy compliance tracking and reporting.

17.6 ACCESS CONTROL

17.6.1 All County workforce members are required to adhere to the access control procedures established by the related agency.

17.6.2 Agency management is responsible for ensuring their staff adheres to access control policy listed above.

17.6.3 All system administrators are responsible to provide the password for a new unique user ID to only the user to whom the new ID is assigned. When a password reset is requested by a user, the system administrator is responsible for verifying the identity of the user or verifying that the person making the request is authorized to request a password reset for another user.

17.7 SYSTEMS DEVELOPMENT AND MAINTENANCE

17.7.1 Users are to be held responsible for all activities that occur while using their assigned application accounts.

17.7.2 Agencies are responsible for monitoring all security-related changes in law and regulations as well as any other legal requirements that may impact the security of a business application. Agencies/departments are to ensure that any required modifications to support legal and regulatory requirements are implemented in a timely manner.

17.7.3 Developers and Users should only use application accounts appropriate to their level of access.

17.8 INCIDENT MANAGEMENT

17.8.1 Each Agency is responsible for fully cooperating in the County's security incident response policy as well as in a common, countywide process designed to mitigate the effects of security incidents.

17.8.2 The IST is involved in the investigation of any Agency-based security incident. The IST is responsible for assigning personnel to specific incident response tasks and for coordinating the overall incident response. In some events, directives given by a member of the IST will supersede this document.

17.8.3 Agency IT staff is responsible for routinely evaluating system logs and other pertinent information for signs of security incidents and for periodically checking security advisory listings and other sources of security alert information.

17.8.4 It is the responsibility of each employee, contractor, vendor, and customer to safeguard information and to report breeches or threats to all County information processing systems.

17.8.5 It is the responsibility of CEO/IT to provide Agencies with incident escalation procedures.

17.9 BUSINESS CONTINUITY AND DISASTER RECOVERY

17.9.1 Agencies are ultimately responsible for development, maintenance, testing and implementation of their respective business continuity and disaster recovery plans.

17.10 COMPLIANCE

17.10.1 Agency management is responsible for ensuring that agency activities are in compliance with the IT Security Policy

17.11 RISK ASSESSMENT AND MITIGATION

17.11.1 The agency identified ISO is responsible for their agency's security programs, including risk management. They play a leading role in introducing an appropriate, structured methodology to identify, evaluate, and minimize risks to the agency.

17.11.2 Local Security Administrators (LSA) are responsible for proper implementation of security requirements on their local IT systems. As those systems change through expansion, maintenance and upgrades, the LSA must support and use the risk assessment and mitigation process to address new security risks and implement new security controls as needed.

17.11.3 System and information owners are responsible for ensuring that proper controls are in place to address the integrity, confidentiality, and availability of the IT systems and data they own. System and information owners are responsible for changes to their IT systems. The system and information owners must therefore understand their role in the risk management process and fully support this process by working with the agency ISO and LSA.

17.12 PRIVACY

17.12.1 All County workforce members are responsible for the security of PII.

18 APPENDIX E: POLICY STATEMENT SOURCES

Policy Section	Source Title	Source Section
1	ISO/IEC 2005:27002	06.1.1 Management commitment to information security
2.2	ISO/IEC 2005:27002	05.1.1: Information Security Policy document
2.2.3	ISO/IEC 2005:27002	05.1.2 Review of the Information Security Policy
2.2.3	ISO/IEC 2005:27002	06.1.8 Independent review of information security
2.2.9	ISO/IEC 2005:27002	08.2.2 Information security awareness, education, and training
3.2.1	ISO/IEC 2005:27002	06.1.2 Information security coordination
3.2.3 3.2.2	ISO/IEC 2005:27002	06.1.3: Define all IS responsibilities
3.2.4	ISO/IEC 2005:27002	06.1.4 Authorization process for information processing facilities
3.2.5	ISO/IEC 2005:27002	06.1.5 Confidentiality agreements
3.2.6 3.2.7	ISO/IEC 2005:27002	06.2.1 Identification of risks related to external parties
3.2.6 3.2.7	ISO/IEC 2005:27002	06.2.2 Addressing security when dealing with customers
3.2.6 3.2.7	ISO/IEC 2005:27002	06.2.3 Addressing security in third party agreements
3.2.7 4.2.6 Appendix D	ISO/IEC 2005:27002	10.02.1 Service delivery
3.2.7 4.2.6 Appendix D	ISO/IEC 2005:27002	10.02.2 Monitoring and review of third party services
3.2.7 4.2.6 6.2.2	ISO/IEC 2005:27002	10.02.3 Managing changes to third party services
4.2.1	ISO/IEC 2005:27002	08.1.2 Screening
4.2.2	ISO/IEC 2005:27002	08.1.3 Terms and conditions of employment
4.2.3	ISO/IEC 2005:27002	08.2.3 Disciplinary process
4.2.4	ISO/IEC 2005:27002	08.3.1: Termination Responsibilities
4.2.4	ISO/IEC 2005:27002	08.3.2: Return of assets
4.2.4	ISO/IEC 2005:27002	08.3.3: Removal of access rights
5.2.1	ISO/IEC 2005:27002	09.1.1 Physical security perimeter
5.2.10 5.2.11	ISO/IEC 2005:27002, NIST SP800-88, NISPOM2006-5220	09.2.6 Secure disposal or re-use of equipment
5.2.2	ISO/IEC 2005:27002	09.1.2 Physical entry controls
5.2.3	ISO/IEC 2005:27002	09.1.4: Protecting against external and environmental threats
5.2.3	ISO/IEC 2005:27002	09.2.1 Equipment citing and protection
5.2.4	ISO/IEC 2005:27002	09.1.3 Securing offices, rooms, and facilities
5.2.4	ISO/IEC 2005:27002	09.1.5 Working in secure areas
5.2.5	ISO/IEC 2005:27002	09.1.6: Public access, delivery/loading areas
5.2.6	ISO/IEC 2005:27002	09.2.2 Supporting utilities
5.2.7	ISO/IEC 2005:27002	09.2.3 Cabling Security

Policy Section	Source Title	Source Section
5.2.8	ISO/IEC 2005:27002	09.2.4 Equipment maintenance
5.2.9	ISO/IEC 2005:27002	09.2.5 Security of equipment off-premises
5.2.9	ISO/IEC 2005:27002	09.2.7 Removal of property
6.2.1	ISO/IEC 2005:27002	10.01.1 Documented operating procedures
6.2.10	ISO/IEC 2005:27002	10.10.5 Fault logging
6.2.11	ISO/IEC 2005:27002	10.06.1 Network controls
6.2.11	ISO/IEC 2005:27002	10.06.2 Security of network services
6.2.12	ISO/IEC 2005:27002	10.07.1 Management of removable media
6.2.12	ISO/IEC 2005:27002	10.07.2 Disposal of media
6.2.13	ISO/IEC 2005:27002	10.07.3 Information handling procedures
6.2.14	ISO/IEC 2005:27002	10.07.4 Security of system documentation
6.2.15	ISO/IEC 2005:27002	10.08.1 Information exchange policies and procedures
6.2.15	ISO/IEC 2005:27002	10.08.2 Exchange agreements
6.2.16	ISO/IEC 2005:27002	10.08.5 Business information systems
6.2.16	ISO/IEC 2005:27002	10.09.1 Electronic commerce
6.2.16	ISO/IEC 2005:27002	10.09.2 On-Line Transactions
6.2.17	ISO/IEC 2005:27002	10.08.4 Electronic messaging
6.2.17.2	ISO/IEC 2005:27002	15.1.4 Data protection and privacy of personal information
6.2.19	ISO/IEC 2005:27002	10.09.3 Publicly available information
6.2.2 - 6.2.2.4	ISO/IEC 2005:27002	10.01.2 Change management
6.2.20	ISO/IEC 2005:27002	10.10.6: Clock synchronization
6.2.21	ISO/IEC 2005:27002	12.6.1 Control of technical vulnerabilities
6.2.22	ISO/IEC 2005:27002	10.08.3 Physical media in transit
6.2.3	ISO/IEC 2005:27002	10.01.3: Segregation of duties
6.2.4	ISO/IEC 2005:27002	10.01.4 Separation of development, test, and operational facilities
6.2.5	ISO/IEC 2005:27002	10.03.1 Capacity management
6.2.6	ISO/IEC 2005:27002	10.03.2 System acceptance
6.2.7	ISO/IEC 2005:27002	10.04.1 Controls against malicious code
6.2.7	ISO/IEC 2005:27002	10.04.2: Control against mobile code
6.2.8	ISO/IEC 2005:27002	10.05.1 Information back-up
6.2.9	ISO/IEC 2005:27002	10.10.1 Audit logging
6.2.9	ISO/IEC 2005:27002	10.10.3 Protection of log information
6.2.9	ISO/IEC 2005:27002	10.10.4 Administrator and operator logs
7.2.1	ISO/IEC 2005:27002	11.1.1: Access Control Policy
7.2.1 7.2.3	ISO/IEC 2005:27002	11.4.1: Policy on use of network services
7.2.1.10	ISO/IEC 2005:27002	11.5.3 Password management system
7.2.1.2 7.2.3	ISO/IEC 2005:27002	11.4.2: User authentication for external connections
7.2.1.3	ISO/IEC 2005:27002	11.5.2 User identification and authentication

Policy Section	Source Title	Source Section
7.2.1.9 7.2.1.10 7.2.1.11	ISO/IEC 2005:27002	11.2.1: User registration 11.2.2: Privilege management 11.2.3: User password management 11.2.4: Review of user access rights
7.2.1.9 7.2.1.10 7.2.1.11	ISO/IEC 2005:27002	11.3.1 Password use
7.2.10	ISO/IEC 2005:27002	11.3.3 Clear desk and clear screen policy
7.2.2	ISO/IEC 2005:27002	11.3.2: Unattended user equipment
7.2.2	ISO/IEC 2005:27002	11.5.5 Session time-out
7.2.2	ISO/IEC 2005:27002	11.5.6 Limitation of connection time
7.2.3	ISO/IEC 2005:27002	11.4.3 Equipment identification in networks
7.2.3	ISO/IEC 2005:27002	11.4.4 Remote diagnostic and configuration port protection
7.2.3	ISO/IEC 2005:27002	11.4.5 Segregation in networks
7.2.3	ISO/IEC 2005:27002	11.4.6 Network connection control
7.2.3	ISO/IEC 2005:27002	11.4.7 Network routing control
7.2.5	ISO/IEC 2005:27002	11.5.4 Use of system utilities
7.2.5	ISO/IEC 2005:27002	11.6.1 Information access restriction
7.2.8	ISO/IEC 2005:27002	11.7.1 Mobile computing and communications
7.2.9	ISO/IEC 2005:27002	11.7.2 Teleworking
8.2.1 - 8.2.5 8.2.14 8.2.15	ISO/IEC 2005:27002	12.1.1: Security requirements analysis and specification 12.2.1: Input data validation 12.2.2: Control of internal processing 12.2.3: Message integrity 12.2.4: Output data validation 12.5.5: Outsourced software development 12.5.4 Information Leakage
8.2.10	ISO/IEC 2005:27002	12.5.1 Change control procedures
8.2.11	ISO/IEC 2005:27002	12.5.2 Technical review of applications after operating system changes
8.2.12	ISO/IEC 2005:27002	12.5.3 Restrictions on changes to software packages
8.2.6	ISO/IEC 2005:27002	12.3.1 Policy on the use of cryptographic controls
8.2.6	ISO/IEC 2005:27002	12.3.2 Key management
8.2.7	ISO/IEC 2005:27002	12.4.1 Control of operational software
8.2.8	ISO/IEC 2005:27002	12.4.2 Protection of system test data
8.2.9	ISO/IEC 2005:27002	12.4.3 Access control to program source code
8.2.1 - 8.2.5 8.2.14 8.2.15	ISO/IEC 2005:27002	12.1.1: Security requirements analysis and specification 12.2.1: Input data validation 12.2.2: Control of internal processing 12.2.3: Message integrity 12.2.4: Output data validation 12.5.5: Outsourced software development 12.5.4 Information Leakage
9.2.1	ISO/IEC 2005:27002	13.2.1 Responsibilities and procedures
9.2.1.1	ISO/IEC 2005:27002	13.1.1 Reporting information security events
9.2.2	ISO/IEC 2005:27002	13.2.2 Learning from information security incidents
9.2.3	ISO/IEC 2005:27002	13.2.3 Collection of evidence

Policy Section	Source Title	Source Section
9.2.6	ISO/IEC 2005:27002	13.1.2 Reporting security weaknesses
9.2.7	ISO/IEC 2005:27002	06.1.6 Contact with authorities
9.2.8	ISO/IEC 2005:27002	06.1.7 Contact with special interest groups
Appx D	ISO/IEC 2005:27002	08.1.1: Roles and responsibilities
Appx D	ISO/IEC 2005:27002	08.2.1 Management responsibilities
10.2.1-10.2.1.3	ISO/IEC 2005:27002	14.1.1 Including information security in the business continuity management process
10.2.1-10.2.1.3	ISO/IEC 2005:27002	14.1.2 Business continuity and risk assessment
10.2.1-10.2.1.3	ISO/IEC 2005:27002	14.1.3 Developing and implementing continuity plans including information security
10.2.1-10.2.1.3	ISO/IEC 2005:27002	14.1.4 Business continuity planning framework
10.2.1-10.2.1.3	ISO/IEC 2005:27002	14.1.5 Testing, maintaining and re-assessing business continuity plans
11.1.1	ISO/IEC 2005:27002	15.1.1 Identification of applicable legislation
11.1.2	ISO/IEC 2005:27002	15.1.2 Intellectual property rights (IPR)
11.2.4	ISO/IEC 2005:27002	15.2.1 Compliance with security policies and standards
11.2.5	ISO/IEC 2005:27002	15.2.2 Technical compliance checking
11.2.6	ISO/IEC 2005:27002	15.3.1: Information systems audit considerations 15.3.2: Protection of information systems audit tools
12.2	ISO/IEC 2005:27002	04.1: Risk Management
12.2	ISO/IEC 2005:27002	04.2: Treating Security Risks
12.2.1	NIST SP800-30	04.1: Risk Management, 04.2: Treating Security Risks

19 APPENDIX F: LEGISLATIVE POLICY DRIVERS

Title	Description
HIPAA (Health Insurance Portability and Accountability Act of 1996): HIPAA Security Rule (2003)	The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services (HHS) to establish national standards for the security of electronic health care information. The final rule adopting HIPAA standards for security was published in the Federal Register on February 20, 2003. This final rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. The standards are delineated into either required or addressable implementation specifications.
California State Civil Code §1798.81	Protection and Disposal of Personal Information
California State Civil Code §1798.82	Disclosure of Security Breech involving Personal Information
California State Civil Code §1798.83	Disclosure of Personal Information to Third-parties
California State Civil Code §1798.84	Explains violations of civil codes §1798.81 - 1798.84
California Senate Bill 1386 (2002)	Amended civil code §1798.82, §1798.84, and added California Notice of Security Breech Law (civil code §1798.29)
California Assembly Bill 1298 (2007)	Amended civil code §1798.29 & §1798.82, to include medical information as personal information

20 APPENDIX G: ACKNOWLEDGEMENT

By signing this document, I acknowledge that I have read, understand and will abide by the County of Orange Information Technology Security Policy.

Employee Name (please print): ____

Employee Signature: ____

Agency/Department: ____

Date: ______________________