



**CONTRACT MA-017-20011143**

**BETWEEN**

**THE COUNTY OF ORANGE**

**AND**

**PRIME GOVERNMENT SOLUTIONS**

**FOR**

**AGENDA MANAGEMENT SYSTEM**

**Table of Contents**

Recitals ..... 3

Articles ..... 3

General Terms and Conditions ..... 3

Additional Terms and Conditions ..... 10

Contract Signature Page ..... 29

Attachment A – Scope of Work ..... 30

Attachment B – Cost Compensation ..... 35

Attachment C – Staffing Plan ..... 39

Attachment D – Implementation Plan, Acceptance, and Testing Procedures ..... 40

Attachment E – Annual Maintenance and Support ..... 41

Attachment F – Solution Delivery Hosted/Managed ..... 42

Attachment G – Business Associate Contract ..... 45

Attachment H – Information Technology Security Policy ..... 46

Attachment I – Prime Government Solutions Service Agreement ..... 47

Attachment J – Prime Government Solutions Service Level Agreement ..... 47

Attachment K – Prime Government Solutions Security Policies and Procedures ..... 48

Appendix 1: OC Agenda Business Requirements and Roadmap ..... 49

Appendix 2: Agenda Database Structure for Data Migration ..... 51

Appendix 3: Sample Feed to Crestron ..... 52

## **Contract MA-017-20011143**

This contract to provide an Agenda Management System (Agenda system) for the County of Orange (“Contract”) is made and entered into as of the date fully executed by and between the County of Orange, a political subdivision of the State of California, acting through the County Executive Office/Office of Information Technology, (“County”) and Prime Government Solutions LLC, with a place of business at 220 N. 1200 E. Suite 201 Lehi, Utah 84043 (“Contractor”). County and Contractor may be referred to individually as a “Party” or collectively as “Parties”.

### **Recitals**

**WHEREAS**, the County conducted Request for Proposal (RFP) OCIT-C015202-TS for an Agenda System; and

**WHEREAS**, the Contractor responded to the RFP and represented that its proposed goods and services shall meet or exceed the requirements and specifications of the RFP.

**NOW, THEREFORE**, the Parties mutually agree as follows:

### **Articles**

#### **General Terms and Conditions**

- A. Governing Law and Venue:** This Contract 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 Contract, 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 Contract:** This Contract contains the entire Contract 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 Purchasing Officer or designee.
- C. Amendments:** No alteration or variation of the terms of this Contract 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. Out-of-state Contractors 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 Contractor.
- E. Delivery:** Time of delivery of goods or services is of the essence in this Contract. County reserves the right to refuse any goods or services and to cancel all or any part of the goods not conforming to applicable specifications, drawings, samples or descriptions or services that do not conform to the prescribed statement of work. Acceptance of any part of the order for goods shall not bind County to accept future shipments nor deprive it of the right to return goods already accepted at Contractor’s expense. Over shipments and under shipments of goods shall be only

as agreed to in writing by County. Delivery shall not be deemed to be complete until all goods or services have been received and meet the acceptance criteria defined in the SOW and/or paragraph 41 "Acceptance Testing".

- F. 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 tested to meet the standard defined in the agreed upon SOW and/or paragraph 41, Acceptance Testing and 2) payment shall be made in accordance with Attachment B, Cost Compensation after satisfactory acceptance.
- G. Warranty:** Contractor expressly warrants that the goods covered by this Contract are 1) free of liens or encumbrances, 2) merchantable and good for the ordinary purposes for which they are used, and 3) fit for the particular purpose for which they are intended. Acceptance of this order shall constitute an agreement upon Contractor's part to indemnify, defend and hold County and its indemnitees as identified in paragraph Z, Indemnification Provision, below, and as more fully described in paragraph Z, Indemnification Provision, harmless from liability, loss, damage and expense, including reasonable counsel fees, incurred or sustained by County by reason of the failure of the goods/services, negligent or unlawful acts, and non-compliance with any applicable state or federal codes, ordinances, orders, or statutes, including the Occupational Safety and Health Act (OSHA) and the California Industrial Safety Act. Such remedies shall be in addition to any other remedies provided by law.
- H. Patent/Copyright Materials/Proprietary Infringement:** Unless otherwise expressly provided in this Contract, Contractor shall be solely responsible for clearing the right to use any patented or copyrighted materials in the performance of this Contract. Contractor 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. Contractor agrees that, in accordance with the more specific requirement contained in paragraph Z, Indemnification Provision, below, it shall indemnify, defend and hold County and County Indemnitees harmless from any and all such claims and be responsible for payment of all costs, damages, penalties and expenses related to or arising from such claim(s), including, costs and expenses but not including attorney's fees.
- I. 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 Contract nor any portion thereof may be assigned by Contractor without the express written consent of County. Any attempt by Contractor to assign the performance or any portion thereof of this Contract without the express written consent of County shall be invalid and shall constitute a breach of this Contract.
- J. Non-Discrimination:** In the performance of this Contract, Contractor 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. Contractor acknowledges that a violation of this provision shall subject Contractor to penalties pursuant to Section 1741 of the California Labor Code.
- K. Termination:** In addition to any other remedies or rights it may have by law, County has the right to immediately terminate this Contract 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 misrepresentation or fraud on the part of the Contractor. Exercise by County of its right to terminate the Contract shall relieve County of all further obligation. In the event County terminates contract without cause there shall be no refunds of prior payments made by County.
- L. Consent to Breach Not Waiver:** No term or provision of this Contract 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.
- M. Independent Contractor:** Contractor shall be considered an independent contractor and neither Contractor, its employees, nor anyone working under Contractor shall be considered an agent or an employee of County. Neither

Contractor, its employees nor anyone working under Contractor shall qualify for workers' compensation or other fringe benefits of any kind through County.

**N. Performance:** Contractor shall warrant all work under this Contract, taking necessary steps and precautions to perform the work to County's satisfaction. Contractor shall be responsible for the professional quality, technical assurance, timely completion and coordination of all documentation and other goods/services furnished by the Contractor under this Contract. Contractor shall perform all work diligently, carefully, and in a good and workmanlike manner; shall furnish all necessary labor, supervision, machinery, equipment, materials, and supplies, shall at its sole expense obtain and maintain all permits and licenses required by public authorities, including those of County required in its governmental capacity, in connection with performance of the work. If permitted to subcontract, Contractor shall be fully responsible for all work performed by subcontractors.

**O. Insurance Provisions:** Prior to the provision of services under this Contract, the Contractor agrees to purchase all required insurance at Contractor's expense, including all endorsements required herein, necessary to satisfy the County that the insurance provisions of this Contract have been complied with. Contractor agrees to keep such insurance coverage, Certificates of Insurance, and endorsements on deposit with the County during the entire term of this Contract. In addition, all subcontractors performing work on behalf of Contractor pursuant to this Contract shall obtain insurance subject to the same terms and conditions as set forth herein for Contractor.

Contractor shall ensure that all subcontractors performing work on behalf of Contractor pursuant to this Contract shall be covered under Contractor's insurance as an Additional Insured or maintain insurance subject to the same terms and conditions as set forth herein for Contractor. Contractor shall not allow subcontractors to work if subcontractors have less than the level of coverage required by County from Contractor under this Contract. It is the obligation of Contractor to provide notice of the insurance requirements to every subcontractor and to receive proof of insurance prior to allowing any subcontractor to begin work. Such proof of insurance must be maintained by Contractor through the entirety of this Contract for inspection by County representative(s) at any reasonable time.

All self-insured retentions (SIRs) shall be clearly stated on the Certificate of Insurance. Any self-insured retention (SIR) in an amount in excess of Fifty Thousand Dollars (\$50,000) shall specifically be approved by the County's Risk Manager, or designee, upon review of Contractor's current audited financial report. If Contractor's SIR is approved, Contractor, in addition to, and without limitation of, any other indemnity provision(s) in this Contract, agrees to all of the following:

- 1) In addition to the duty to indemnify and hold the County harmless against any and all liability, claim, demand or suit resulting from Contractor's, its agents, employee's or subcontractor's performance of this Contract, Contractor shall defend the County at its sole cost and expense with counsel approved by Board of Supervisors against same; and
- 2) Contractor's duty to defend, as stated above, shall be absolute and irrespective of any duty to indemnify or hold harmless; and
- 3) The provisions of California Civil Code Section 2860 shall apply to any and all actions to which the duty to defend stated above applies, and the Contractor's SIR provision shall be interpreted as though the Contractor was an insurer and the County was the insured.

If the Contractor fails to maintain insurance acceptable to the County for the full term of this Contract, the County may terminate this Contract.

#### **Qualified Insurer**

The policy or policies of insurance must be issued by an insurer with a minimum rating of A- (Secure A.M. Best's Rating) and VIII (Financial Size Category as determined by the most current edition of the **Best's Key Rating Guide/Property-Casualty/United States or ambest.com**). It is preferred, but not mandatory, that the insurer be licensed to do business in the state of California (California Admitted Carrier).

If the insurance carrier does not have an A.M. Best Rating of A-/VIII, the CEO/Office of Risk Management retains the right to approve or reject a carrier after a review of the company's performance and financial ratings.

The policy or policies of insurance maintained by the Contractor shall provide the minimum limits and coverage as set forth below:

Coverage	Minimum Limit
Commercial General Liability	\$1,000,000 per occurrence \$2,000,000 aggregate
Automobile Liability including coverage for owned, non-owned and hired vehicles	\$1,000,000 per occurrence
Workers Compensation	Statutory
Employers Liability Insurance	\$1,000,000 per occurrence
Network Security & Privacy Liability	\$1,000,000 per claims-made
Technology Errors & Omissions	\$1,000,000 per claims-made \$1,000,000 aggregate

### Required Coverage Forms

The Commercial General Liability coverage shall be written on Insurance Services Office (ISO) form CG 00 01, or a substitute form providing liability coverage at least as broad.

The Business Auto Liability coverage shall be written on ISO form CA 00 01, CA 00 05, CA 0012, CA 00 20, or a substitute form providing coverage at least as broad.

### Required Endorsements

The Commercial General Liability policy shall contain the following endorsements, which shall accompany the Certificate of Insurance:

- 1) An Additional Insured endorsement using ISO form CG 20 26 04 13 or a form at least as broad naming the *County of Orange its elected and appointed officials, officers, agents and employees* as Additional Insureds, or provide blanket coverage, which will state **AS REQUIRED BY WRITTEN CONTRACT**.
- 2) A primary non-contributing endorsement using ISO form CG 20 01 04 13, or a form at least as broad evidencing that the Contractor's insurance is primary and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

The Network Security and Privacy Liability policy shall contain the following endorsements which shall accompany the Certificate of Insurance:

- 1) An Additional Insured endorsement naming the County of Orange, its elected and appointed officials, officers, agents and employees as Additional Insureds for its vicarious liability.
- 2) A primary and non-contributing endorsement evidencing that the Contractor's insurance is primary and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

The Workers' Compensation policy shall contain a waiver of subrogation endorsement waiving all rights of subrogation against the *County of Orange, its elected and appointed officials, officers, agents and employees* or provide blanket coverage, which will state **AS REQUIRED BY WRITTEN CONTRACT**.

All insurance policies required by this Contract shall waive all rights of subrogation against the County of Orange, its elected and appointed officials, officers, agents and employees when acting within the scope of their appointment or employment.

Contractor shall notify County in writing within thirty (30) days of any policy cancellation and ten (10) days for non-payment of premium and provide a copy of the cancellation notice to County. Failure to provide written notice of cancellation may constitute a material breach of the Contract, upon which the County may suspend or terminate this Contract.

If Contractor's Professional Liability, Technology Errors & Omissions and/or Network Security & Privacy Liability are "Claims-Made" policy(ies), Contractor shall agree to maintain coverage for two (2) years following the completion of the Contract. (Only include this provision when Professional Liability, Technology Errors & Omissions and/or Network Security & Privacy Liability Insurance are required. Only reference the type(s) of insurance required in the contract.)

The Commercial General Liability policy shall contain a severability of interests clause also known as a "separation of insureds" clause (standard in the ISO CG 0001 policy).

Insurance certificates should be forwarded to the department address listed on the Contract.

If the Contractor fails to provide the insurance certificates and endorsements within seven (7) days of notification by OCIT Contracts & Procurement Division.

County expressly retains the right to require Contractor to increase or decrease insurance of any of the above insurance types throughout the term of this Contract. Any increase or decrease in insurance will be as deemed by County of Orange Risk Manager as appropriate to adequately protect County.

County shall notify Contractor in writing of changes in the insurance requirements. If Contractor does not deposit copies of acceptable Certificates of Insurance and endorsements with County incorporating such changes within thirty (30) days of receipt of such notice, this Contract may be in breach without further notice to Contractor, and County shall be entitled to all legal remedies.

The procuring of such required policy or policies of insurance shall not be construed to limit Contractor's liability hereunder nor to fulfill the indemnification provisions and requirements of this Contract, nor act in any way to reduce the policy coverage and limits available from the insurer.

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

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

County reserves the right to immediately terminate the Contract 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 Contract.

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

The Contractor shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with County interests. In addition to the Contractor, this obligation shall apply to the Contractor's employees, agents, and subcontractors associated with the provision of goods and services provided under this Contract. The Contractor'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.

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

**S. Confidentiality:** Contractor shall ensure the confidentiality, protection and preservation of the County's Confidential Information (defined below) and information of a confidential, sensitive, and/or proprietary nature, which may be disclosed or made available to Contractor for its performance of services under this Contract, all related subordinate agreements, and its cyber security assessment and audit of the County's network equipment, and associated software, information and documentation (collectively, the "Purpose"). Confidential Information means all non-public information, material, or documents, of any kind obtained from, or on behalf of, the County through any medium that is:

- i. Designated in writing as "confidential" or "private" at the time of its disclosure; or
- ii. The County's sensitive security information, technical data, programs, software (including configuration or source codes), technical information, screen shots, customer information, employee records, computer network, or architectural or engineering information; or
- iii. Exploitable data, information protected by privacy law, or other information that is treated as confidential by the County, or is prohibited from being disclosed for any reason pursuant to law, statute, regulation, ordinance, or contract; or
- iv. Any County information security record the disclosure of which would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of the County; or
- v. Information obtained by Contractor and relating to the County during Contractor's performance of the Contract, any related subordinate agreements, or the Purpose, that a reasonable person knows or reasonably should understand to be confidential and is treated confidential by the disclosing party.

"Confidential Information" means non-public information, technical data or know-how of a party and/or its Affiliates, which is furnished to the other party in written or tangible form in connection with this Contract. Oral disclosure will also be deemed Confidential Information if it would reasonably be considered to be of a confidential nature or if it is confirmed at the time of disclosure to be confidential.

Confidential Information does not include information which is: (i) already in the possession of the receiving party and not subject to a confidentiality obligation to the providing party; (ii) independently developed by the receiving party; (iii) publicly disclosed through no fault of the receiving party; (iv) rightfully received by the receiving party from a third party that is not under any obligation to keep such information confidential; (v) approved for release by written agreement with the disclosing party; or (vi) disclosed pursuant to the requirements of law, regulation, or court order, provided that the receiving party will promptly inform the providing party of any such requirement and cooperate with any attempt to procure a protective order or similar treatment.

Neither party will use the other party's Confidential Information except as reasonably required for the performance of this Contract. Each party will hold in confidence the other party's Confidential Information by means that are no less restrictive than those used for its own confidential materials. Each party agrees not to disclose the other party's Confidential Information to anyone other than its employees or subcontractors who are bound by confidentiality obligations and who need to know the same to perform such party's obligations hereunder. The confidentiality obligations set forth in this clause will survive for five (5) years after the termination or expiration of this Contract.

Upon termination or expiration of this Contract, except as otherwise agreed in writing or otherwise stated in this Contract, each party will, upon the request of the disclosing party, either: (i) return all of such Confidential



Information of the disclosing party and all copies thereof in the receiving party's possession or control to the disclosing party; or (ii) destroy all Confidential Information and all copies thereof in the receiving party's possession or control. The receiving party will then, at the request of the disclosing party, certify in writing that no copies have been retained by the receiving party, its employees or agents.

In case a party receives legal process that demands or requires disclosure of the disclosing party's Confidential Information, such party will give prompt notice to the disclosing party, if legally permissible, to enable the disclosing party to challenge such demand.

- T. Compliance with Laws:** Contractor represents and warrants that services to be provided under this Contract shall fully comply, at Contractor's expense, with all 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. Contractor acknowledges that County is relying on Contractor to ensure such compliance, and pursuant to the requirements of paragraph Z, Indemnification Provision, below, Contractor agrees that it shall defend, indemnify and hold County and County Indemnitees harmless from all liability, damages, costs, and expenses arising from or related to a violation of such laws.
- U. Freight (F.O.B. Destination):** Prior to the County's express acceptance of delivery of products. Contractor assumes full responsibility for all transportation, transportation scheduling, packing, handling, insurance, and other services associated with delivery of all products deemed necessary under this Contract.
- V. Severability:** If any term, covenant, condition, or provision of this Contract 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.
- W. Attorney Fees:** In any action or proceeding to enforce or interpret any provision of this Contract, or where any provision hereof is validly asserted as a defense, each party shall bear its own attorney's fees, costs and expenses.
- X. Interpretation:** This Contract has been negotiated at arm's length and between persons sophisticated and knowledgeable in the matters dealt with in this Contract. In addition, each party has been represented by experienced and knowledgeable independent legal counsel of their 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 they have not been influenced to any extent whatsoever in executing this Contract 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 Contract against the party that has drafted it is not applicable and is waived. The provisions of this Contract shall be interpreted in a reasonable manner to affect the purpose of the parties and this Contract.
- Y. Employee Eligibility Verification:** The Contractor 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 Contract meet the citizenship or alien status requirement set forth in Federal statutes and regulations. The Contractor 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. The Contractor shall retain all such documentation for all covered employee, consultants and subcontractors for the period prescribed by the law. The Contractor 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 the Contractor 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 Contract.
- Z. Indemnification Provision:** Contractor agrees to indemnify, defend with counsel approved in writing by County, and hold County, its elected and appointed officials, officers, employees, agents and those special districts and agencies which County's Board of Supervisors acts as the governing Board ("County Indemnitees") harmless from any claims, demands or liability of any kind or nature, including but not limited to personal injury or property

damage, arising from or related to the services, products or other performance provided by Contractor pursuant to this Contract. If judgment is entered against Contractor and County by a court of competent jurisdiction because of the concurrent active negligence of County or County Indemnitees, Contractor and County agree that liability will be apportioned as determined by the court. Neither party shall request a jury apportionment.

- AA. Audits/Inspections:** Contractor agrees to permit the County's Auditor-Controller or the Auditor-Controller's authorized representative (including auditors from a private auditing firm hired by the County under a non-disclosure agreement with Contractor) access during normal working hours to applicable books, accounts, records, reports, files, financial records, supporting documentation, including payroll and accounts payable/receivable records, and other papers or property of Contractor for the purpose of auditing or inspecting any aspect of performance under this Contract. The inspection and/or audit will be confined to those matters connected with the performance of the Contract including, but not limited to, the costs of administering the Contract. The County will provide reasonable notice of such an audit or inspection and such date will be mutually agreed upon.

The County reserves the right to audit and verify the Contractor's records before final payment is made.

Contractor 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 Contract or by law. Contractor agrees to allow interviews of any employees or others who might reasonably have information related to such records. Further, Contractor agrees to include a similar right to the County to audit records related to performance of this Contract.

Should the Contractor cease to exist as a legal entity, the Contractor'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.

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

## Additional Terms and Conditions

### Definitions

- a. Acceptance Criteria.** The term "Acceptance Criteria" shall have the meaning set forth in Paragraph 41.
- b. Acceptance Testing.** The term "Acceptance Testing" shall have the meaning set forth in Paragraph 41.
- c. Annual Maintenance and Support.** The term "Annual Maintenance and Support" shall mean the services set forth in Attachment E of the Contract.
- d. Annual Maintenance and Support Period.** The term "Annual Maintenance and Support Period" shall mean the twelve (12) month consecutive period commencing on the Contract term start date as defined in Paragraph 1, Term of Contract, below. Each successive "Annual Maintenance and Support Period" shall commence at 12:00 a.m. (PT) midnight of the calendar day of the expiration of the prior period.
- e. Availability.** The term "Availability" shall mean the percentage of time that a given Service or System is fully operational and available when its resources are called upon at a random point in time. Availability represents a measure of the fraction of time (expressed as a percentage) during a defined period when the Service or System is deemed to be equal to or better than a Designated Service Level.  
  
Availability measurement calculations shall be limited to those Service and System components that are directly under control of the Contractor, as well as Service and System components for which the Contractor is responsible for subcontracting to third parties.
- f. BOS.** The term "BOS" shall mean the County of Orange Board of Supervisors.

- g. Business Day.** The term “Business Day” or “business day”, whether capitalized or not and unless expressly specified otherwise, shall mean any day on which the County of Orange is open for business.
- h. CAPS+.** The term “CAPS+” shall mean the central accounting software system for the County. CAPS+ is based on Oracle database and web-based User Interface.
- i. Calendar Day.** The term “Calendar Day” or “calendar day”, whether capitalized or not and unless expressly specified otherwise, shall mean any day of the week, month or year.
- j. CEO.** The term “CEO” shall mean the County of Orange County Executive Office.
- k. Change(s).** The term “Change(s)” or “change(s)”, whether capitalized or not and unless expressly specified elsewhere, shall mean any change, modification, action or decision with respect to the Services or the Systems.
- l. Commercial Hardware.** The term “Commercial Hardware” shall mean Hardware developed or regularly used that: (i) has been sold, leased, or licensed to the general public; (ii) has been offered for sale, lease or license to the general public; (iii) has not been offered, sold, leased, or licensed to the public but will be available for commercial sale, lease, or license in time to satisfy the delivery requirements of this Contract; or (iv) satisfies a criterion expressed in (i), (ii), or (iii) above and would require only minor modifications to meet the requirements of this Contract.
- m. Commercial Software.** The term “Commercial Software” shall mean Software developed or regularly used that: (i) has been sold, leased, or licensed to the general public; (ii) has been offered for sale, lease or license to the general public; (iii) has not been offered, sold, leased, or licensed to the public but will be available for commercial sale, lease, or license in time to satisfy the delivery requirements of this Contract; or (iv) satisfies a criterion expressed in (i), (ii), or (iii) above and would require only minor modifications to meet the requirements of this Contract.
- n. Consent.** The term “Consent” or “consent”, whether capitalized or not and unless expressly specified otherwise, shall mean, with regard to either a specified or an applicable Party whose consent is required hereunder, the voluntary, freely-given approval of such Party, which may be withheld in such Party’s sole discretion, with no duty to be reasonable in the withholding of such approval.
- o. County Data.** The term “County Data” shall have the meaning set forth in Paragraph 29.
- p. Deliverable.** The term “Deliverable” shall mean tangible and intangible information or material that must be provided by the Contractor to the County under the terms of this Contract.
- q. Data Loss Prevention.** The term “Data Loss Prevention” shall mean the strategy used to ensure sensitive or critical data is not transmitted outside of the system.
- r. Documentation.** The term “Documentation” shall mean, with respect to any particular items: (i) all of the written, printed, electronic, or otherwise formatted materials that relate to such items, or any component thereof; (ii) all user, operator, system administration, technical, training, support, and other manuals and all other written, printed, electronic, or other format materials that represent, demonstrate, explain or describe the functional, operational or performance capabilities of such items; and (iii) all specifications, materials, flow charts, notes, outlines, manuscripts, writings, pictorial or graphical materials, schematics, and other documents that represent, demonstrate, explain or describe such items.
- s. Go Live.** The term “Go Live” shall mean the milestone in Attachment B where the Contractor provides the County with written notice that the Agenda system is ready to be used by the County.
- t. Agenda system.** The term “Agenda system” shall mean Agenda Management System.
- u. Effective Date.** The term “Effective Date” shall mean the date that Contract is fully executed by all parties.
- v. End User.** The term “End User” or “end user”, whether capitalized or not and unless expressly specified elsewhere, shall mean the person upon whom the County intends to confer the right to access and use the Agenda system or receive the benefit of the Agenda system.

- w. **Equipment.** The term “Equipment” shall mean either individual machine or the complete data processing System.
- x. **Hardware.** The term “Hardware” shall mean computer Equipment and is contrasted with Software.
- y. **Incident.** The term “Incident” shall mean any event which is not part of the standard operation of a Service and which causes, or may cause, an interruption to, or a reduction in, the quality of that Service.
- z. **Including.** The term “Including” or “including”, whether capitalized or not and unless expressly specified otherwise, shall mean “including, but not limited to.”
- aa. **Integration.** The term “Integration” shall mean to link together different systems and/or applications, either physically or functionally.
- bb. **Malware.** The term “Malware” shall mean software designed to infiltrate or damage a computer system without the owner's informed consent. Software is considered Malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, crime ware and other malicious and unwanted software.
- cc. **Owner-Centric.** The term “Owner-Centric” shall mean a project information system that allows owners to measure and manage every step of the capital project delivery process from planning, design, procurement, construction and operations including capital program costs, schedule, and documents utilizing workflow and business intelligence.
- dd. **Service(s).** The term “Service(s)” shall mean the work or labor being performed or already performed in accordance with this Contract.
- ee. **Service Level/Service Level Requirements.** “Service Level” means, generally, a minimum acceptable level of service or performance for a particular task, activity, or Service performed by Contractor hereunder, as specified in Attachments B and J. “Service Level Requirements” or “SLR” is the specific performance requirement for a Service Level (typically, but not exclusively, a measure of efficiency expressed as a percentage).
- ff. **SOC (Service Organization Controls) Reports for Service Organizations**
  - A. SOC 1 Report — Report on Controls at a Service Organization Relevant to User Entities Internal Control over Financial Reporting (SSAE 16).
  - B. SOC 2 Report— Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy.
  - C. SOC 3 Report— Trust Services Report for Service Organizations.

Source:  
<http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/serviceorganization'smanagement.aspx>
- gg. **Software.** The term “Software” shall mean computer programs and program objects of any kind (including object code and source code, and any intermediate forms or versions thereof), program set-up and customization parameters and data, and the tangible media on which any of the foregoing are recorded.
- hh. **System.** The term “System” shall mean a set of interacting or independent components forming an integrated whole providing a business process.
- ii. **TLS.** The term “TLS” shall mean Transport Layer Security.
- jj. **Update.** The term “Update” shall mean any bugs, patches, fixes, enhancements, improvements to the Software and any addition of new features pertaining only to the County’s existing modules.

- kk. Upgrade.** The term “Upgrade” shall mean platform changes, addition of new modules or new integration points or the creation of new versions.
- ll. U.S. Intellectual Property Rights.** The term “U.S. Intellectual Property Rights” shall mean intellectual property rights enforceable in the United States of America, including without limitation rights in trade secrets, trademarks, copyrights, and U.S. patents.
- mm. Workaround.** The term “Workaround” shall mean a temporary solution that the Contractor or the County can implement in the event of an Incident as an alternate method of providing full Service or process functionality that allows the affected System(s) and/or process(s) to deliver to the County an acceptable level of business operations functionality until the Incident is resolved. Any such Workaround must be acceptable to and approved by the County.
1. **Term of Contract:** The Term of the Contract is for three (3) years beginning May 7, 2020 through and including May 6, 2023. The Contract may be renewed for a total of two (2) consecutive two-year periods under the same terms and conditions and pricing structure by written consent of both Parties. The County does not have to give any reason should it elect not to renew the Contract. Any renewal may require approval of the County of Orange Board of Supervisors.
  2. **Scope of Contract:** This Contract specifies the contractual terms and conditions by which the County will procure an Agenda System from Contractor as further detailed in the Scope of Work, identified and incorporated herein by this reference as Attachment A.
  3. **Compensation:** The Contractor agrees to accept the compensation as set forth in Attachment B, Cost Compensation, as full remuneration for (a) performing all Services and furnishing all staffing and materials required, (b) any reasonably unforeseen difficulties which may arise or be encountered in the performance of the Services until acceptance, (c) risks connected with the Services, and (d) performance by the Contractor of all its duties and obligations required herein.
  4. **Taxes:** This Contract shall include any and all applicable taxes. The Contractor certifies all taxes applicable to the Services and/or products in this Contract are hereby outlined in Attachment B, Cost Compensation. The County shall not be charged or liable for any taxes not specified. The Contractor shall bear the full responsibility and shall be liable for full payment (or full reimbursement to the County) of any Local, State, and/or Federal taxes not outlined in Attachment B, Cost Compensation.
  5. **Fiscal Appropriations:** This Contract 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 forthcoming, the Contract shall be terminated without penalty. The Contractor acknowledges that funding or portions of funding for this Contract may also be contingent upon the receipt of funds from, and/or appropriation of funds by, the State of California to the County. If such funding and/or appropriations are not forthcoming, or are otherwise limited, the County may immediately terminate or modify this Contract without penalty.
  6. **Waiver of Rights:** Any action or inaction by the County or the failure of the County on any occasion, to enforce any right or provision of the Contract, shall not be construed to be a waiver by the County of its rights hereunder and shall not prevent the County from enforcing such provision or right on any future occasion. The rights and remedies of the County herein are cumulative and are in addition to any other rights or remedies that the County may have at law or in equity.
  7. **No Third-Party Beneficiaries:** This Contract is an agreement by and between the Parties, and neither: (a) confers any rights upon any of the employees, agents, or contractors of either Party, or upon any other person or entity not a party hereto; or (b) precludes any actions or claims against, or rights of recovery from, any person or entity not a party hereto.
  8. **Employee Qualification Verification:** Subject to and in accordance with applicable law, the Contractor, prior to assigning an individual as the Contractor personnel and at the Contractor’s sole expense, shall have appropriately verified the qualifications of such individual, including verifying employment history, conducting reference checks,

verifying non-employer technical certifications or education completed or degrees awarded, performing drug testing, and a security background check that includes investigation and identification of all state or federal misdemeanor or felony convictions of such individual, and criminal charges pending against such individual, during the immediately preceding seven (7) years, and performing such other types of verification as reasonably requested by the County. On request from the County, the Contractor will certify in writing to the County that each and every employee of the Contractor and any subcontractor working on the County's account or having access to County Data meets all employee qualifications required in this Contract and under law. Failure to provide such certification constitutes a material breach of this Contract.

9. **Training:** The Contractor shall provide, and cause its subcontractors to provide throughout the Term of this Contract, all such technical and interpersonal training to the Contractor personnel, and to any employees of the Contractor's subcontractors that are assigned to provide Services hereunder, as may be necessary and appropriate for them to collectively perform, on behalf of the Contractor, all of the Contractor's duties under this Contract. In any event, the levels and extent of training provided by the Contractor to the Contractor personnel shall be at least equal to the average levels of training given to other Contractor employees holding comparable positions, under similar circumstances, and performing work of a similar nature and level of complexity.
10. **Non-Solicitation of Employees:** Except as otherwise expressly provided in this Contract, during the Term and for the first twelve (12) months thereafter, neither Party shall, without the prior written consent of the other Party, directly or indirectly solicit, entice, encourage, or otherwise recruit any employee of such other Party whose duties and responsibilities include performing Services directly or indirectly connected with performance under this Contract to leave such other Party's employ in order to accept employment or other engagement with the soliciting Party, its affiliates, or any other person. Notwithstanding the foregoing, the Parties acknowledge and agree that this Contract shall not prohibit solicitations by either Party through general advertising or other publications of general circulation. In no way is this clause intended, nor shall it be deemed, to restrict or limit any individual's right to seek employment, but rather this clause is intended to, and shall, prevent each Party from actively recruiting the employees of the other Party (except as provided in this Contract), thereby depriving such other Party of vital resources in the securing, development, training, and deployment of whom it has expended considerable time and resources.
11. **Authority Retained by County:** The County shall have and at all times retain the exclusive right and authority to: (a) define, determine, and control the County's Agenda system-related policies, strategies, objectives, and goals; (b) define, determine, and alter any or all of the County's business processes; and (c) assess the Contractor's quality and performance. The Contractor shall, at all times during the Term, perform and provide the Services in accordance with the strategies, processes, and policies described in the immediately preceding sentence, subject to the terms of this Contract.
12. **Set-Off:** The County may set-off against any and all amounts otherwise payable to the Contractor pursuant to any of the provisions of this Contract: (i) any and all amounts claimed by the County in good faith to be owed by the Contractor to the County pursuant to any of the provisions of this Contract; and (ii) any and all amounts claimed by the County in good faith to be owed by the Contractor pursuant to any other written agreement between the Parties. Within twenty (20) days after any such set-off by the County, the County shall provide the Contractor with a written accounting of such set-off and a written statement of the reasons therefore.
13. **Disputed Amounts:** The County may withhold payment of fees or any other charges otherwise due to the Contractor under this Contract to the extent that the County disputes such charges in good faith. In such case, the County shall provide to the Contractor a detailed written explanation of the basis for the dispute and shall continue to make payments of undisputed amounts as otherwise provided in this Contract. If any disputed amounts are later determined to have been improperly withheld (i.e., properly charged by the Contractor), then the County shall be obligated to pay the withheld amount in accordance with this Contract, until paid in full. If any paid amounts are later disputed by the County and determined to have been improperly paid (i.e., improperly charged by the Contractor), then the Contractor shall promptly pay the County, in cash, the improperly paid amount. The failure of the County to withhold payment shall not waive any other rights the County may have with respect to disputed amounts or overpayments. Except as

otherwise provided herein, any dispute relating to amounts owed by a Party hereunder, shall be considered a disagreement.

14. **Non-Exclusivity:** Nothing herein shall prevent the County from providing for itself or obtaining from any third party, at any time during the Term or thereafter, the Services, or any type of products or services in any way analogous, similar, or comparable to the Services, as applicable, or any other products or services. Nor shall anything in this Contract be construed or interpreted as limiting the County's right or ability during the Term to increase or decrease its demand for Services hereunder.
15. **Software License:** Unless otherwise specified in the Scope of Work, the Contractor hereby grants to the County and the County accepts from the Contractor, subject to the terms and conditions of this Contract, an irrevocable, royalty-free, non-exclusive, license to use all Software of any type provided by Contractor to County.
16. **Future Releases:** Unless otherwise specifically provided in this Contract, or the Scope of Work, if improved versions, e.g., patches, bug fixes, Updates or releases, of any solution are developed by the Contractor, and are made available to other licensees, they will be made available to the County at no additional cost only if such are made available to other licensees at no additional cost. If the Contractor offers new versions or Upgrades to the solution, they shall be made available to the County at the County's option at a price no greater than the Contract price plus a price increase proportionate to the increase from the list price of the original version to that of the new version, if any. If the Software product has no list price, such price increase will be proportionate to the increase in average price from the original to the new version, if any, as estimated by the Contractor in good faith.
17. **Software Maintenance:** The correction of any residual errors in any software products which may be discovered by the Contractor or by the County will be considered maintenance. Such maintenance will be performed by the contractor without additional charge for the duration of this Contract. The contractor will be available to assist the County in isolating and correcting error conditions caused by the County's particular hardware or operating system at rates specified in this contract. If the contractor is called upon by the state to correct an error caused by the County's negligence, modification by the County, County-supplied data, or machine or operator failure or due to any other cause not inherent in the original software products, the contractor reserves the right to charge the County for such service on a time and material basis at rates in accordance with the contract.
18. **Legal Entity:** Should the Contractor cease to exist as a legal entity, the Contractor's records pertaining to this Contract shall be forwarded to the surviving entity in a merger or acquisition or, in the event of liquidation, to the County's Project Manager.
19. **Breach:** The failure of the Contractor to comply with any of the provisions, covenants, requirements or conditions of this Contract shall be a material breach of this Contract. In such event, the County may, in addition to any other remedies available at law, in equity, or otherwise specified in this Contract, do any of the following:
  - a. Afford the Contractor written notice of the breach and, if the breach is curable, sixty (60) calendar days after receiving such notice, within which the Contractor is to cure the breach;
  - b. Discontinue payment to the Contractor for and during the period in which the Contractor is in breach;
  - c. Offset against any monies billed by the Contractor but yet unpaid by the County those monies disallowed pursuant to above section 20 a, b, and d; and
  - d. Terminate the Contract immediately. Upon notice of termination for breach, Contractor shall immediately return all County Data to the County in Coma Separated Value file format.
20. **Orderly Termination:** Upon ending of the Term, termination or other expiration of this Contract, 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 this Contract. In addition, each Party shall assist the other Party in orderly termination of this Contract and the transfer of all assets, tangible and intangible, as may be necessary for the orderly, non-disruptive business continuation of each Party. No less than thirty (30) days prior to the expiration date of this Contract, the Contractor shall return all County Data to the County in Coma Separated Value file format.

21. **County and Contractor Project Manager:** The County shall appoint a Project Manager to act as liaison between the County and the Contractor during the term of this Contract, as described in Paragraph 22, County's Project Manager. The Contractor shall appoint a Project Manager to direct the Contractor's efforts in fulfilling the Contractor's obligations under this Contract and who will ensure that County personnel interface with the Contractor personnel in a manner conducive to facilitating the Contractor's performance of the Services under this Contract, including the timely evaluation and testing of the Services, as described in Paragraph 41, Acceptance Testing. The Contractor's Project Manager shall not be changed without the written notice to the County's Project Manager. The County's Project Manager shall have the right to request the removal and replacement of the Contractor's Project Manager from providing Services to the County under this Contract. The County's Project Manager shall notify the Contractor in writing of such action. The Contractor shall have five (5) business days to review the request either remedy the situation to the County's satisfaction or appoint an interim Project Manager. If an interim Project Manager is appointed, Contractor shall have twenty (20) business days to appoint a permanent Project Manager.
22. **County's Project Manager:** The County represents that the individual designated as the County's Project Manager is, and shall ensure that any replacement holder of such position shall be, an experienced manager who is knowledgeable as to the County, its respective businesses, business practices, functions, and related activities, and its respective systems, requirements, and needs. The County's Project Manager shall at all times: (a) act as the primary liaison between the County and the Contractor's Project Manager; (b) have overall responsibility for directing and coordinating all of the County's activities hereunder; and (c) be vested with the necessary authority to fulfill all of the responsibilities of the County's Project Manager described in this clause.
23. **Contractor Staff:** In addition to the rights set forth in Paragraph 21, County and Contractor Project Manager, above, the County's Project Manager shall have the right to request the removal and replacement of any of the Contractor's personnel from providing Services to the County under this Contract. The County's Project Manager shall notify the Contractor's Project Manager in writing of such request. The Contractor shall make reasonable effort to either remedy the situation to the County's satisfaction or remove and replace with new personnel within five (5) business days after written notice by the County's Project Manager.
24. **Contractor's Project Manager:** The Contractor represents that the individual designated as the Contractor's Project Manager is and promises that any replacement holder of such position shall be, an experienced manager who is knowledgeable as to the solution, requirements, and needs. The Contractor's Project Manager shall at all times: (i) act as the primary liaison between the Contractor and the County's Project Manager; (ii) have overall responsibility for directing all of the Contractor's activities hereunder, including directing the performance of all Services from inception through completion; (iii) be vested with the necessary authority to fulfill all of the responsibilities of the Contractor's Project Manager described in this Contract; and (iv) coordinate and conduct periodic program review sessions with the County to discuss costs, Attachments, and any relevant technical aspects of the Contractor's performance under this Contract.
25. **Qualified Contractor Staff:** The Contractor shall, at all times, make available appropriate and sufficient numbers and types of qualified Contractor personnel, in addition to the Contractor's Project Manager, to timely perform the Contractor's obligations hereunder, in accordance with this Contract. In the event that the Contractor fails to meet any of its obligations with respect to the required proficiency of any Contractor personnel, the Contractor shall promptly, as directed by the County, either: (a) take such action with respect to such Contractor personnel, including promptly providing appropriate training, education, or orientation, as necessary for such Contractor personnel to meet the applicable requirements set forth in this paragraph; or (b) in the event that the County has notified the Contractor that such Contractor personnel does not meet the applicable requirements, remove and replace such Contractor personnel with an appropriately qualified individual, in accordance with this Contract, and such position shall be filled by a qualified person no later than thirty (30) days following the date of removal or replacement.



26. **Reports/Meetings:** The Contractor shall develop reports and any other relevant documents necessary to complete the Services and requirements as set forth in this Contract. The County's Project Manager and the Contractor's Project Manager shall meet on reasonable notice to discuss the Contractor's performance and progress under this Contract. If requested by the County, the Contractor's Project Manager and other project personnel shall attend (either in person or remotely) County meetings. The Contractor shall provide such information that is requested by the County for the purpose of monitoring progress under this Contract.
27. **Documentation:** The Contractor agrees to provide to the County, at no charge, all Documentation as described within the Scope of Work, and updated versions thereof, which are necessary or useful to the County in its use of the solution provided hereunder. The Contractor agrees to provide additional Documentation at prices not in excess of charges made by the Contractor to its other customers for similar Documentation.
28. **Conflict of Interest – (Contractor):** The Contractor shall exercise reasonable care and diligence to prevent any actions or conditions that result in a conflict with the best interests of the County. This obligation shall apply to the Contractor; the Contractor's employees, agents, relatives, sub-tier contractors; and third parties associated with accomplishing work and Services hereunder. The Contractor's efforts shall include, but are not limited to, establishing precautions to prevent its employees or agents from making, receiving, providing or offering gifts, entertainment, payments, loans or other considerations which could be deemed to appear to influence individuals to act contrary to the best interest of the County.
29. **County Data:** Subject to applicable law, the County shall permit the Contractor and its subcontractors to have access to, and make appropriate use of, the information or material that the County submits to the Contractor pursuant to this Contract ("County Data"), solely to the extent the Contractor requires such access and use in order to properly and appropriately perform the Services as contemplated by this Contract. The Contractor may only access and use County Data in connection with performance of its duties under this Contract or as specifically directed by the County in writing and may not otherwise use, disclose, modify, merge with other data, commercially exploit, or make any other use of County Data or take, or refrain from taking, any other action that might, in any manner or form, adversely affect or jeopardize the integrity, security, or confidentiality of County Data, except as expressly permitted herein or as expressly directed by the County in writing. The Contractor acknowledges and agrees that, as between the Parties, the County owns all right, title, and interest in, and all Intellectual Property Rights in and to, all County Data.
30. **Ownership by the County:** All County Data, reports and other documents or materials created by the County through its use of the Agenda System, including all Intellectual Property Rights in or pertaining to the same, shall be owned solely and exclusively by the County. The Parties further agree that all materials, documents, data or information obtained from the County or any County medium furnished to the Contractor in the performance of this Contract shall 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 the Contractor after completion or termination of this Contract without the express written consent of the County. All materials, documents, data or information, including copies, must be returned to the County upon expiration of the Term or termination of this Contract.

As the Parties agree that the County shall always own the County Data, the County expressly agrees to have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use of all of County Data. Except for the Contractor's material breach of County Data, the Contractor shall take appropriate technical and organizational measures against unauthorized or unlawful processing of, and accidental loss or destruction of, or damage to, Personal Data, having regard to the state of technological development and the cost of implementing any measures, to ensure a level of security appropriate to the harm that might result from such unauthorized or unlawful processing, accidental loss, destruction or damage and the nature of the Personal Data; only process Personal Data in accordance with instructions from the County and the County shall not provide the Contractor access to sensitive personal information that imposes specific security data security obligations for the processing of such data.; and take reasonable steps to ensure the reliability of its employees who have access to the Personal Data.

31. **Conditions Affecting Work:** The Contractor shall be responsible for taking all steps reasonably necessary to ascertain the nature and location of the work to be performed under this Contract and to reasonably know the general conditions which can affect the work or the cost thereof. Any unreasonable failure by the Contractor to do so shall not relieve the Contractor from responsibility for successfully performing the work without additional cost to the County. The County assumes no responsibility for any understanding or representations made by any of its officers or agents during or prior to the execution of this Contract concerning the nature, location(s) or general conditions of the Contract, unless such understanding or representations by the County are expressly stated in the Contract and the Contract expressly provides that the County assumes the responsibility.
32. **Contractor's Expense:** The Contractor will be responsible for all costs related to photocopying, telephone communications, fax communications, travel, parking, and any and all "out of pocket" expenses incurred by the Contractor during the performance of the Services under this Contract, unless otherwise specified. The Contractor shall be responsible for payment of all parking costs and expenses incurred at a County facility while performing work under this Contract, except to the extent the County facility has free parking available to the public and the Contractor makes appropriate use of this free parking. However, the County will at no point provide free parking to the Contractor in the County Civic Center.
33. **Gratuities:** The Contractor warrants that no gratuities, in the form of entertainment, gifts or otherwise, were offered or given by the Contractor or any agent or representative of the Contractor to any officer or employee of the County with a view toward securing the Contract or securing favorable treatment with respect to any determinations concerning the performance of the Contract. For breach or violation of this warranty, the County shall have the right to terminate the Contract, 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 the Contractor agreed to supply shall be borne and paid for by the Contractor. 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 Contract.
34. **Authorization Warranty:** The Contractor represents and warrants that the person executing this Contract on behalf of and for the Contractor is an authorized agent who has actual authority to bind the Contractor to each and every term, condition and obligation of this Contract and that all requirements of the Contractor have been fulfilled to provide such actual authority.
35. **News/Information Release:** The Contractor agrees that it shall not issue any news releases in connection with either the award of this Contract or any subsequent amendment of or effort under this Contract without first obtaining review and written approval of said news releases from the County through the County's Project Manager.
36. **Publication:** No copies of sketches, schedules, written documents, computer based data, photographs, maps or graphs, including graphic art work, resulting from performance or prepared in connection with this Contract, are to be released by the Contractor and/or anyone acting under the supervision of the Contractor to any person, partnership, company, corporation, or agency, without prior written approval by the County, except as necessary for the performance of the Services under this Contract. All press releases, including graphic display information to be published in newspapers, magazines, etc., are to be administered only by the County unless otherwise agreed to by both Parties.
37. **Errors and Omissions:** All reports, files and other documents prepared and submitted by the Contractor shall be complete and shall be carefully checked by the professional(s) identified by the Contractor as Project Manager and key personnel attached hereto, prior to submission to the County. The Contractor agrees that County review is discretionary, and the Contractor shall not assume that the County shall discover errors and/or omissions. If the County discovers any errors or omissions prior to approving the Contractor's reports, files and other written documents, the reports, files or other written documents shall be returned to the Contractor for correction. Should the County or others discover errors or omissions in the reports, files or other written documents submitted by the Contractor after County approval thereof, the County approval of the Contractor's reports, files or other written documents shall not be used as a defense by the Contractor in any action between the County and the Contractor, and the reports, files or other written documents shall be returned to the Contractor for correction.

38. **OEM Equipment Maintenance Standard:** The Contractor agrees to maintain all equipment according to the original equipment manufacturer (OEM) specifications. The Contractor further agrees that all components shall be OEM components. At the termination of the Contract, the Contractor guarantees that the equipment shall meet OEM equipment certification standards.
39. **Security Deliverables and Documents:** As this Contract may involve the Contractor having direct access to County proprietary information, IT staff, and Systems, the County has outlined various Deliverables and Documentation in relation to Contractor data security that shall be provided by the Contractor to the County within thirty (30) calendar days prior to going live. The County shall review these Deliverables and Documentation prior to final approval and actual access to the resources or transfer of any information related to this Contract.

Deliverables and Documentation to be provided by the Contractor are as follows:

a. Staff Related Items

- Pre-Employment Screening Policy/Procedure
- Background Check Procedure
- Staff Roster and Duties
- US Staffing Duties

b. Security Related Items

- SOC 1 Type I or Type II report (within twelve (12) months of report date but no older than twenty-four (24) months). If the report is not provided the Contractor agrees to provide a SOC 1 Type II report upon County's request at Contractor's expense within 180 days of County request.

c. I.T. Systems Related Items

- Policies and Procedures Related to Data, Tapes, and Resources that will be removed from County Facility
- Policies and Procedures Related to Access to County Data Internally or Via Remote Access

40. **Relationship Management:**

- a. Status Reports: Periodically during the Term of this Contract, but not less frequently than once each month, the Contractor shall be responsible for identifying, analyzing, managing and recording issues and risks throughout the Implementation period and will provide the County with an action plan for resolution. The Contractor shall deliver to the County Project Manager a written report summarizing the progress of the Services and the operation of the Agenda system during the preceding month, including problems that have occurred and that could delay the Contractor's performance of anticipated activities and expected problems during the upcoming month (each such report, a "Status Report"). At a minimum, each Status Report shall include: (a) the current status and progress of the performance of the Services and an assessment of how such status and progress compares to the deadlines set forth in the Scope of Work; (b) any actual delays; (c) any reasonably anticipated delays; (d) any failures, or correction of any failures; and (e) such other information as the County may reasonably request from time to time. Notwithstanding the foregoing, the Contractor shall immediately notify (but in no event more than five (5) business days after the Contractor first knew of such obstruction or delay) the County's Project Manager, in writing, in the event that the Contractor is materially obstructed or delayed in its performance of the Services.
- b. Status Meetings: During the Term, representatives of the Parties shall meet and/or teleconference periodically as requested by the County to discuss matters arising under this Contract. The place and time, and whether to meet via teleconference or in person, shall be as determined as mutually agreed upon by the Parties.

- c. Action Plan: The Contractor shall be responsible for identifying, analyzing, managing and recording issues and risks throughout the Implementation period and will provide the County with an action plan for resolution.

41. **Acceptance Testing**: All Deliverables shall be provided to the County by the Contractor in conformity with all requirements, specifications, Acceptance Criteria, and time periods set forth or referenced in this Contract. The Contractor shall at all times utilize complete and thorough Acceptance Testing Procedures, and appropriate Acceptance Criteria, all of which shall be subject to review and approval in mutual agreement by the County's Project Manager and Contractor's Project Owner, and no such activities shall be deemed completed until all Acceptance Criteria, whether set forth in this Contract or mutually agreed upon by the Parties in writing, have been successfully met. Moreover, nothing in this section shall limit in any way the County's right to terminate immediately for cause pursuant to Paragraph K, Termination, herein.

- a. Acceptance Testing: Following the Contractor's notification to the County that the Contractor has completed any component or Deliverable identified in this Contract, at a mutually agreed scheduled time thereafter, the County shall begin testing the component or Deliverable to determine whether such component or Deliverable conforms to the applicable specifications and/or standards (collectively, the "Acceptance Criteria"). After the County has completed such testing or upon expiration of the agreed-upon testing period or any agreed-upon extension of the testing period (the "Acceptance Testing Period"), the County shall notify the Contractor in writing either that the component or Deliverable: (a) meets the Acceptance Criteria and that acceptance of such component or Deliverable has occurred ("Acceptance"); or (b) does not meet the Acceptance Criteria and the reasons therefor. If the component or Deliverable is identified as being part of a larger, integrated system being developed thereunder, then any Acceptance under the terms of this subsection shall be understood as being conditional acceptance ("Conditional Acceptance"), and such component or Deliverable shall be subject to Final Acceptance, as described below.
- b. Cure: If the County determines that a component or Deliverable does not conform to the applicable Acceptance Criteria, and that it is in the County's interest to allow the Contractor time to correct the problem, the County shall deliver to the Contractor a written exception report describing the nonconformity (the "Exception Report"). Within ten (10) calendar days following receipt of the Exception Report, the Contractor shall: (a) perform a Root Cause Analysis to identify the cause of the nonconformity; (b) provide the County with a written report detailing the cause of, and procedure for correcting, such nonconformity; (c) provide the County with satisfactory evidence that such nonconformity will not recur; and (d) use best efforts to correct critical errors (as determined by the County) and use commercially reasonable efforts to correct all other errors reasonably requested by the County and accepted by the Contractor; provided, however, that if the nonconformity of critical errors is incapable of cure within such ten (10) calendar day period then, within such ten (10) calendar day period, the Contractor shall present to the County a mutually agreeable plan to cure such nonconformity within a reasonable amount of time. Upon the Contractor's notice to the County that the Contractor has cured any such nonconformity, the County shall re-test the defective component or Deliverable for an additional testing period of up to thirty (30) calendar days or such other period as the Parties may mutually agree upon in writing, at the end of which period the process described in subsections (a) through (c) above shall be repeated. In the event the County rejects the component or Deliverable a second time and the Contractor disagrees with such rejection, then the Parties shall escalate the issue(s) to senior management of both Parties for mutual resolution.
- c. Final Acceptance: Upon achievement of Conditional Acceptance for all identified components or Deliverables, the County shall begin testing the System that is comprised of such components or Deliverables using the applicable test procedures and standards to determine whether such System performs as an integrated whole in accordance with the Acceptance Criteria. After the County has completed such testing or upon expiration of the testing period (the "Final Acceptance Testing Period"), the County shall notify the Contractor in writing that the System, and all components and Deliverables that are a part thereof: (a) meet the Acceptance Criteria and that final acceptance of the System and such components and Deliverables has occurred ("Final Acceptance"); or (b) does not meet the Acceptance Criteria and the reasons therefor. If the County determines that the Acceptance Criteria have not been so met, the process described in subsection (b) above shall be initiated, with all references to "component or Deliverable" being references to the "System," and all references

to the "Acceptance Testing Period" being references to the "Final Acceptance Testing Period." Neither Conditional Acceptance, Acceptance nor Final Acceptance by the County shall constitute a waiver by the County of any right to assert claims based upon defects not discernible through conduct of the applicable test procedures and subsequently discovered in a component or Deliverable or the System following the County's Final Acceptance thereof. Nothing else, including the County's use of the System, or any component thereof, shall constitute Final Acceptance, affect any rights and remedies that may be available to the County and/or constitute or result in "acceptance" under general contract law, any state uniform commercial code or any other law.

42. **Information Technology Policies and Procedures:** The Contractor, its subcontractors, the Contractor personnel, and all other agents and representatives of the Contractor, will at all times comply with and abide by all policies and procedures of the County that are provided or made available to the Contractor that reasonably pertain to the Contractor in connection with the Contractor's performance under this Contract. The Contractor shall cooperate with the County in ensuring the Contractor's compliance with the County policies and procedures described in this Contract and as adopted by the County from time-to-time, and any material violations or disregard of such policies or procedures shall, in addition to all other available rights and remedies of the County, be cause for termination of this Contract.

**Security Policies:** All performance under this Contract shall be in accordance with the County's security requirements, policies, and procedures set forth in this Paragraph 42 and in Attachment H, County of Orange Information Technology Security Policy as it now exists or may hereafter be modified, supplemented, or replaced by the County from time to time, in its sole discretion, by providing the Contractor 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"). The Contractor 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 the County systems accessed in the performance of services in this Contract.

**Information Access:** The Contractor shall, at all times, use appropriate safeguard and security measures so as to ensure the confidentiality and security of all County Data. At all times during the Term, the Contractor shall, and shall cause the Contractor personnel and subcontractors, and the employees or agents of any of the foregoing to, fully comply with all of the County's policies and procedures regarding data access and security, including those prohibiting or restricting remote access to the Agenda System and County Data, as set forth in the Security Policies. The Contractor shall, and shall cause the Contractor personnel and subcontractors to, fully comply with and abide by all such Security Policies at all times during the Term. County may require all Contractor personnel performing Services under this Contract 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 the Contractor shall issue, any necessary information-access mechanisms, including access IDs and passwords, and in no event shall the Contractor permit any such mechanisms to be shared or used by other than the individual Contractor person to whom issued. The Contractor shall provide each Contractor person with only such level of access as is required for such individual to perform his or her assigned tasks and functions. All County Resources (including County systems), and all data contained therein, including County Data, used or accessed by Contractor personnel: (a) shall be used and accessed by such Contractor personnel solely and exclusively in the performance of their assigned duties in connection with, and in furtherance of, the performance of the Contractor's obligations hereunder; and (b) shall not be used or accessed except as expressly permitted hereunder, or commercially exploited in any manner whatsoever, by the Contractor, the Contractor personnel or any subcontractor, at any time. The Contractor acknowledges and agrees that any failure to comply with the provisions of this clause shall constitute a breach of this Contract and entitle the County to deny or restrict the rights of such non-complying Contractor personnel to access and use the system(s) and County Data, as the County in its sole discretion shall deem appropriate.

**Data Security Requirements:** Without limiting Contractor's obligation of confidentiality as further described in this Contract, Contractor shall establish, maintain, and enforce a data privacy and information security program, including safety and physical and technical security policies and procedures, with respect to its processing of County

Data that comply with the requirements of Contractor's data security policies set forth in Attachment K, Prime Government Solutions Security Policies and Procedures, and, to the extent such practices and standards are consistent with and not less protective than the foregoing requirements, are at least equal to applicable best industry practices and standards. Contractor also shall provide technical and organizational safeguards against accidental, unlawful, or unauthorized access to or use, destruction, loss, alteration, disclosure, transfer, commingling, or processing of such information that ensure a level of security appropriate to the risks presented by the processing of County Data, consistent with best industry practice and standards. Further, Contractor shall take all reasonable measures to secure and defend all locations, equipment, systems, and other materials and facilities employed in connection with the Services against "hackers" and others who may seek, without authorization, to disrupt, damage, modify, access or otherwise use Contractor Systems or the information found therein; and prevent County Data from being commingled with or contaminated by the data of other customers or their users of the Services and unauthorized access to any of County Data. Contractor shall also continuously monitor its systems for potential areas where security could be breached. In no case shall the safeguards of Contractor's data privacy and information security program be less stringent than the safeguards used by County. Without limiting any other audit rights of County, County shall have the right to review Contractor's data privacy and information security program prior to commencement of Services and from time to time during the term of this Contract.

**Enhanced Security Measures:** The County may, in its discretion, designate certain areas, facilities, or systems as ones that require a higher level of security and access control. The County shall notify the Contractor 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 the Contractor shall be required to implement and enforce, as well as the date on which such procedures and measures shall take effect. The Contractor shall, and shall cause the Contractor personnel and subcontractors to, fully comply with and abide by all such enhanced security and access measures and procedures as of such date.

**General Security Standards:** At all times during the Term, the Contractor shall maintain a level of security with regard to the Agenda System and County Data for which the Contractor has agreed in this Contract to provide or manage physical security, that in all events is at least as secure as each of the following levels of security: (a) that are maintained by the Contractor with regard to its own systems, data, and facilities of a similar nature and import; and (b) that are common and prevalent in the industry and in accordance with industry best practices.

**Breach of Security:** Any material breach or violation by the Contractor or its subcontractors, or the employees or agents of any of the foregoing, of the Security Policies, shall be deemed a material breach of a material obligation of the Contractor under this Contract, and any chronic or critical breach by the Contractor or its subcontractors, or the employees or agents of any of the foregoing, of the Security Policies, shall be deemed an incurable and material breach of a material obligation of the Contractor under this Contract, which may result in an immediate termination by the County for cause, pursuant to Section K herein.

**Security Breach Notification:**

In the event Contractor becomes aware 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 by Contractor that relate to the security, confidentiality, or integrity of County Data, Contractor 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. Contractor shall reasonably reimburse County for all notification related costs (all such reasonable costs shall be negotiated and agreed upon by the Parties) incurred by County arising out of or in connection with any such occurrence due to Contractor’s acts, errors or omissions, negligence, and/or misconduct resulting in a requirement for legally required notifications.

<p>Rafael Linares                  Chief Information Security Officer                  1055 N. Main Street                  Santa Ana, CA 92701                  Office: (714) 567-7611                  E-mail: <a href="mailto:Rafael.linares@ocit.ocgov.com">Rafael.linares@ocit.ocgov.com</a></p>	<p>Linda Le, CHPC, CHC, CHP                  County Privacy Officer                  1055 N. Main Street                  Santa Ana, CA 92701                  Office: (714) 834-4082                  Email: <a href="mailto:linda.le@ocit.ocgov.com">linda.le@ocit.ocgov.com</a>                  AND  <a href="mailto:securityadmin@ocit.ocgov.com">securityadmin@ocit.ocgov.com</a></p>
---	---

43. **Security Audits:** The County may perform security reviews and testing. Such testing shall ensure all pertinent County security standards are in place. Contractor shall reasonably cooperate with all County security reviews and testing, including but not limited to penetration testing of any cloud-based solution provided by Contractor to County under this Contract. Contractor shall inform County of any security audit or assessment performed by Contractor or at Contractor’s behest or direction that includes County hosted content, within sixty (60) calendar days of such audit or assessment.

44. **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 paper copy delivered by United States mail or hand to Party. 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.

<p>For Contractor:                  Attn: Sherif Agib                  Title: Chief Operations Officer                  Phone 1: 831.261.1660                  Phone 2: (801) 341-1910                  Email: <a href="mailto:sherif@primegov.com">sherif@primegov.com</a></p>
---

<p>For County:                  County of Orange, Information Technology                  Attn: Sue Stock, Project Manager                  714-567-5023                  1055 N. Main Street                  Santa Ana, CA 92701  <a href="mailto:Sue.Stock@ocit.ocgov.com">Sue.Stock@ocit.ocgov.com</a></p>
--

For County:

County of Orange, Information Technology

Attn: Tim Shears, Deputy Purchasing Agent

714-567-7488

1055 N. Main Street

Santa Ana, CA 92701

[Timothy.Shears@ocit.ocgov.com](mailto:Timothy.Shears@ocit.ocgov.com)

45. **Equal Employment Opportunity:** The Contractor shall comply with Executive Order 11246, “Equal Employment Opportunity”, as amended by Executive order 11375, “Amending Executive Order 11246 relating to Equal Employment Opportunity”, and as supplemented by regulations at 41 CFR part 60, “Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor.”
46. **Civil Rights:** The Contractor 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.
47. **Lobbying:** On best information and belief, the Contractor certifies no federal appropriated funds have been paid or will be paid by, or on behalf of, the Contractor to any person for influencing or attempting to influence an officer or employee of Congress; or an employee of a member of Congress in connection with the awarding of any federal contract, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.
48. **Debarment:** The Contractor certifies that neither the Contractor nor its principles are presently debarred, proposed for debarment, declared ineligible or voluntarily excluded from participation in the transaction by any Federal department or agency.
49. **Service Level Commitment:** Except as otherwise specified in this Contract, from and after the Effective Date, the Contractor shall perform the Services at levels that are equal to or better than the Service Level Requirements (“SLR”) applicable to such Services. The Contractor shall be responsible for meeting or exceeding the applicable SLRs even where doing so is dependent on the provision of Services by subcontractors or other non-contractor personnel. The Service Level methodology applicable to the SLRs is set forth in Attachment J – Prime Government Solutions Service Level Agreement and Attachment B – Cost Compensation. Any resources utilized by the Contractor pursuant to the terms hereof shall incorporate methods permitting measurement of all performance-related SLRs. The Contractor shall measure and compare the actual or observed performance resulting from the Contractor’s performance of the Services with the SLRs during each month.
50. **Monitoring and Measuring Tools and Processes:** The Contractor shall implement measurement and monitoring tools and produce the metrics and reports necessary to measure its performance against any of the SLRs and shall deliver to the County such reports in accordance with the frequency set forth in Attachment J – Prime Government Solutions Service Level Agreement. Upon request in connection with an audit, and at no additional charge to the County, the Contractor shall provide the County or its designees with information and access to tools and procedures used to produce such metrics.

**Root Cause Analysis, Predictive Analysis and Resolution:**



- a. Process: Upon the Contractor's discovery of, or, if earlier, the Contractor's receipt of a notice from the County in respect of,
- (i) The Contractor's failure to meet a SLR, or
  - (ii) The Contractor's failure to provide the Services, or to operate, support, and maintain the solution, in accordance with the SLRs and this Contract,

The Contractor shall comply with and follow the processes established in Attachment J – Prime Government Solutions Service Level Agreement concerning Contractor Service Levels. The correction of any such failure shall be performed entirely at the Contractor's expense.

Pending Disputes: Unless otherwise directed by the County, and notwithstanding the pendency of any disagreement or Root Cause Analysis as to the cause of a defect, malfunction, or difficulty, the Contractor shall take prompt and reasonable steps to correct such defect, malfunction, or difficulty at its sole cost.

51. **Compatibility of Resources:** The Contractor shall ensure that the solution Software, all Services, and all Software, assets, Hardware, Equipment, and other resources and materials (collectively, the "Contractor Resources") that are provided by the Contractor to the County, otherwise utilized by the Contractor, or approved by the Contractor for utilization by the County, in connection with the use or operation of the solution, or with the providing or receiving of the Services, shall be successfully and fully integrated and interfaced, and shall be compatible, with, all applicable County Software, Services, Systems, items, and other resources (collectively, the "County Resources") that are owned by or leased or licensed to the County, or that are provided to the County by third party service providers. To the extent that any interfaces need to be developed or modified in order for the Contractor Resources to integrate fully and successfully and be compatible with the County Resources, the Contractor shall be responsible for the development or modification of such interfaces and for such integration, and all such activities shall be deemed to be Services within the scope of this Contract.
52. **Service Level Fee Reductions:** Failure by the Contractor to meet the Application Performance and Service Level guarantees as stated in Attachment J – Prime Government Solutions Service Level Agreement will result in the Fee Reductions stated in Attachment B – Cost Compensation. The Parties agree that the Fee Reductions reflect the diminished value of the Services as a result of Contractor failure to provide the Services in accordance with Attachment J – Prime Government Solutions Service Level Agreement and, accordingly do not constitute nor shall be construed or interpreted as penalties. Fee Reductions shall in no event be the sole and exclusive remedy of County with respect to any failure of the Contractor as described in this clause. Fee Reductions shall be in the form of a credit to the County to be applied to the following invoice. The Contractor shall provide a corrective action plan no later than seventy-two (72) hours of identification of performance issues.
53. **Data Location:** Except where the Contractor obtains the County's prior written approval, the physical location of the Contractor's data center where County Data is stored shall be within the United States.
54. **Security Management Services:** The Contractor shall provide appropriate and comprehensive security Services, that meet the County's security requirements as required by this Contract and in Attachment F – Solution Delivery Hosted/Managed, using industry best practices and methods, and commercially available technology, to at all times ensure the security and integrity of the Agenda system and County Data, and to protect against unauthorized access to, use of, or intrusion into, the Systems and unauthorized disclosure of the County Data. Without limiting anything set forth in the Scope of Work, such Services shall include operating Agenda system under a best practices-based security plan that conforms in all respects to the requirements of all applicable federal, state and local laws, regulations, and ordinances relating to security, privacy, or confidentiality, ensuring compliance with County and County security policies and procedures provided or made available to the Contractor, performing all necessary and appropriate security-related audits and reports, and promptly providing the County with a full and complete copy of each such report.

55. **Anti-Malware Protections:** The Contractor's data center shall have strong access controls and secure practices, such as specialized authorization system(s), in effect at all times to prevent unauthorized physical and virtual access to hosted County systems. The Contractor servers and network equipment hosted at the data center shall be properly secured from the threat of cyber hackers and viruses through appropriate intrusion detection tools, proactive 24x7x365 monitoring and prompt installation of new software updates, hot fixes and security patches.

The Contractor shall use industry best practices regularly to identify, screen, and prevent any Disabling Device in resources utilized by the Contractor in connection with the provision or receipt of the Services and shall not itself knowingly or intentionally install (and shall prevent its subcontractors from knowingly and intentionally installing) any Disabling Device in resources utilized by the Contractor, the County, or any subcontractor, in connection with the provision or receipt of the Services. A "Disabling Device" is a computer virus, timer, clock, counter, time lock, time bomb, or other limiting design, instruction, or routine that would purposely and inappropriately erase data or programming or cause any resource to become inoperable or otherwise incapable of being used in the full manner for which such resource was intended to be used, and any device that may be used as a host to access County Data or launch attacks on the solution.

The Contractor shall assist the County in reducing and mitigating the effects of any Disabling Device discovered in any resource related to the provision or receipt of the Services, especially if such Disabling Device is causing a loss of operating efficiency or data. Timers, clocks, counters, and time locks included as part of any Commercial Software, used by the County, by the manufacturer of that Software shall not be considered Disabling Devices for purposes of this clause.

56. **Disaster Recovery Plan:** The Contractor shall maintain a disaster recovery plan in effect throughout the Term of the Contract. The Disaster Recovery Plan shall be completed and made available for County's review no later than three (3) months after the Contract execution date. The disaster recovery plan shall be subject to the County's review upon reasonable notice to the Contractor. The Contractor shall maintain reasonable safeguards against the destruction, loss, intrusion and unauthorized alteration of printed materials and data in its possession. At a minimum, the Contractor shall perform (i) incremental daily back-ups, (ii) weekly full backups, and (iii) such additional back-ups and other measures the Contractor may determine to be necessary to maintain such reasonable safeguards (collectively herein "Disaster Recovery Plan").

The County's Project Manager may identify and notify the Contractor in writing of other items that the County's Project Manager reasonably deems appropriate for inclusion in the Disaster Recovery Plan. Contractor shall promptly review and discuss with the County's Project Manager all such additional items and, unless the County's Project Manager agrees otherwise in writing, promptly revise the Disaster Recovery Plan to properly address such additional items. In addition, prior to each anniversary of the Effective Date, Contractor shall revise the Disaster Recovery Plan as appropriate to reflect any changes to the County's Agenda system, or related requirements, and submit such revised Disaster Recovery Plan to the County's Project Manager for review, comment, and approval. Contractor shall also periodically (not less than once per Agreement Year) test the procedures set forth in the Disaster Recovery Plan to ensure that Contractor is capable of promptly and successfully executing them. Contractor shall promptly provide the County's Project Manager access to such report summarizing the results of each such test and promptly take appropriate action to cure all deficiencies, and resolve all problems, that are discovered as a result of each such test, performing re-testing as necessary to ensure that such cures and resolutions are effective. Any material breach or material violation by Contractor of its obligations regarding execution of the Disaster Recovery Plan during a disaster shall be deemed an incurable and material breach of this Agreement by Contractor.

57. **Preparation for Successor to this Contract:** At any time or times during the Term, at the written request of the County, the Contractor shall provide the County with any information that the County is entitled to receive under this Contract that the County desires to use in preparing a request for proposal to solicit responses, or responding to proposals, for the purpose of entering into an agreement that would constitute the successor to this Contract. Such requested information may include, among other things, current and projected transactional or other relevant volumes, resource utilization and performance statistics and trends, forms utilization, and such other information,

statistics, and materials related to the provision of the Services or the use, operation, support, and maintenance of the Agenda System as the County shall reasonably deem necessary or appropriate.

58. **Source Code and Contractor's Insolvency:**

In the event Contractor becomes insolvent or bankrupt, Contractor will grant to the County a nonexclusive, nontransferable license for access and use to Contractor's Agenda System Source Code and documentation for the use restricted by this contract.

County agrees:

a) That no copies of the Source Code in any form will be given by the County to any third party except as expressly permitted under the terms of this Contract or required by law, except that access or use by the County or its subcontractors (if any) solely for the purposes of maintaining, upgrading, modifying, or enhancing the Agenda System Software shall be permitted;

b) To reproduce Contractor's copyright notice on all material related to or part of the Contractor's Agenda System on which any such copyright notice is displayed, including any copies made pursuant to this Contract;

c) Not to remove any copyright notices, trademark credits, confidentiality notice, mark, legend, or other information included in the Contractor's Agenda System; and

d) Not to purport to sell, transfer, or assign any intellectual property rights or other rights in or to the Contractor's Agenda System except as expressly permitted by this Contract.

59. **Transition Period:**

a) No less than thirty (30) days prior to the expiration date of this Contract, the Contractor shall assist the County in extracting and/or transitioning all County Data in the format determined by the County ("Transition Period"). All transition services outside of the scope of paragraph 20, Orderly Termination, will be charged to the County on a time and materials basis.

b) The Transition Period may be modified in the Scope of Work or as agreed upon in writing by the Parties in a contract amendment.

c) During the Transition Period, Service and Data access shall continue to be made available to the County without alteration as long as the County is in full compliance with payment for the service.

d) Unless otherwise stated in the Scope of Work, the Contractor shall permanently destroy or render inaccessible any portion of the Data in the Contractor's possession or control following the expiration of all obligations in this clause. Within thirty (30) days, the Contractor shall issue a written statement to the County confirming the destruction or inaccessibility of County Data.

e) The County, at its option, may purchase additional transition services listed in the Scope of Work.

60. **Discovery:** The Contractor shall promptly notify the County upon receipt of any requests which in any way might reasonably require access to County Data or the County's use of the Contractor's Services. The Contractor shall notify the County by the fastest means available and also in writing, with additional notification provided to the County Project Manager or designee, unless prohibited by law from providing such notification. The Contractor shall provide such notification within forty-eight (48) hours after the Contractor receives the request. The Contractor shall not respond to subpoenas, service of process, Public Records Act requests, and other legal requests directed at the Contractor regarding this Contract without first notifying the County, unless prohibited by law from providing such notification. The Contractor agrees to provide its intended responses to the County with adequate time for the County to review, revise and, if necessary, seek a protective order in a court of competent jurisdiction. The Contractor shall not respond to legal requests directed at the County unless authorized in writing to do so by the County.

61. **Contingency Amount Use Request Process:** County may at any time request Contractor to perform additional services related to the Services described in Attachment A – Scope of Work, pursuant to the Contingency Amount Use Request Process outlined in this paragraph.
- a. County’s Project Manager shall submit a written request to Contractor’s Project Manager that specifies the desired services to the same degree of specificity as in the original Scope of Work.
  - b. Contractor shall, not more than thirty (30) business days (or other mutually agreed upon period) after receiving the written request, notify County whether or not the requested services are possible and, if possible, has an associated impact to cost and/or schedule and, if so, provide a firm proposal that specifies the associated impact to the cost and/or schedule of the original Scope of Work.
  - c. If not possible, Contractor and County shall mutually agree upon an alternative scope of work or decide that the additional services are no longer requested.
  - d. Contractor will continue performing the Services in accordance with the current Attachment A – Scope of Work, until both Parties otherwise agree to the requested services.
  - e. If County accepts Contractor’s proposal, Contractor shall provide the requested services for the cost stated in the proposal and subject to the terms and conditions of this Contract.
62. **Precedence:** The Contract documents will consist of this Contract, including its Attachments, Exhibit’s, and Appendices. In the event of a conflict or inconsistency between or among the Contract documents, the following order of precedence shall apply: the provisions of the main body of this Contract, Attachments A – H, Attachments I – k, and then the Appendices.
63. **Refund/Advance Payment:** Should the Contract be terminated with cause prior to the expiration date, Contractor shall promptly refund to County one twelfth (1/12) of the Annual Recurring Fees paid in advance, for the terminated services for each month remaining in the Contract period, which shall be computed based upon the date of written notice of termination.

*The rest of this page intentionally left blank*

**Contract Signature Page**

The Parties hereto have executed this Contract on the dates shown opposite their respective signatures below

**PRIME GOVERNMENT SOLUTIONS LLC\*:**

By: Sherif Agib Digitally signed by Sherif Agib Date: 2020.03.17 14:30:57 -07'00' Title: Chief Operations Officer

Print Name: Sherif Agib Date: 3-17-2020

By: Jason Byrne Digitally signed by Jason Byrne Date: 2020.03.17 21:44:39 Z Title: Chief Financial Officer

Print Name: Jason Byrne Date: 3-17-2020

*\*If the contracting party is a corporation, two (2) signatures are required: one (1) signature by the Chairman of the Board, the President or any Vice President; and one (1) signature by the Secretary, any Assistant Secretary, the Chief Financial Officer or any Assistant Treasurer. The signature of one person alone is sufficient to bind a corporation, as long as he or she holds corporate offices in each of the two categories described above. For County purposes, proof of such dual office holding will be satisfied by having the individual sign the instrument twice, each time indicating his or her office that qualifies under the above described provision.*

*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

By: \_\_\_\_\_ Title: \_\_\_\_\_

Print Name: \_\_\_\_\_ Date: \_\_\_\_\_

Approved by Board of Supervisors on: \_\_\_\_\_

**APPROVED AS TO FORM  
OFFICE OF THE COUNTY COUNSEL,**

By:   
Deputy

## Attachment A – Scope of Work

### I. OVERVIEW

The County of Orange (“County”) is seeking to implement an Agenda Management (“Agenda system”) System specifically designed to meet the needs of the County of Orange, Office of the Clerk of the Board (COB), the County Executive Office (CEO), and over 20 other County Agencies and Departments.

### II. BACKGROUND

The County’s existing Agenda system is a mission-critical system that manages the Board of Supervisors’ (BOS) agenda process. The current Agenda system allows the County to manage the four stages of the Agenda system process lifecycle:

1. **Creation** of ASRs, including originating, review, approval, and submission by County departments;
2. **Compiling** ASR’s, including reviewing, processing, and agenda publishing based upon the submitted ASRs and mandated filing instructions;
3. **Recording** and publishing actions taken by the BOS during meetings; and
4. **Archiving** transmittal and agenda documents with retrieval access by for future reference and research by County employees and constituents.

The current Agenda system comprises three sub-systems: CAMS, Agenda Works, and the Agenda Search Engine.

#### 1. CAMS (Comprehensive Agenda Management System)

CAMS is the first component of the current Agenda system. It is a web-based system used by County Agencies and Departments to manage the process of preparing, approving, and submitting ASRs and other official documents for BOS meetings. Once an ASR is submitted, it goes through a workflow/approval process. Each workflow/approval process is defined and tailored to each of the 26 Departments and five Board offices. Each of the 26 Departments and 5 Board offices has its own approval structure of groups, group membership, approval queues and order of execution. Each also has mandatory approval steps along with optional approval steps based on the responses entered in the ASR.

#### 2. Agenda Works

Agenda Works is the second component of the current Agenda system. It is a client-based system the COB uses to finalize and publish/distribute BOS meeting agendas, including ASRs, minutes, resolutions, and other official documents. The Agenda Works component compiles and uploads the processed agenda and associated documents to the appropriate website. This component also creates CD for distribution.

#### 3. Agenda Search Engine

The Agenda Search Engine is the third component of the current Agenda system. It was recently developed and launched to provide County-wide access to BOS agendas that have been published, including ASRs, minutes, resolutions, and other official documents.

The existing system provides data feeds to the Crestron system and to the Video Broadcast System. The Crestron System is used for the BOS touch-screen monitors installed at the dais. This feed is an output file in text format with proper line breaks/formatting and saved to a specific location when the Agenda system is published. The Video Broadcast System receives a copy of the final agenda (including any revisions and/or supplemental agenda items) from the Agenda system in a standard format to allow the agenda to be posted prior to the BOS meeting being broadcasted.

The Agenda system will be a fully managed Software-as-a-Service (SaaS) solution hosted by the Contractor that is configurable to meet all of the County’s business requirements as described in Appendix 1 which outlines agreed upon

Contractor product roadmap detailing items and timelines included within this Contract entitled “OC Agenda Business Requirements and Roadmap”.

### III. CONTRACTOR RESPONSIBILITIES

#### A. Application Interoperability

Contractor’s Agenda system solution shall:

1. Be a SAAS system that is a fully configurable COTS system capable of interfacing with other County systems for data exchange, including, but not limited to, the following systems:
  - Crestron system – The Agenda system shall provide an automated electronic data feed to the Crestron system that complies with the current feed’s file structure in text format. A sample of this feed is provided in Appendix 2, Sample Feed to Crestron system. The Agenda system shall create and save this feed to a specific location when the agenda is published. Every time an agenda is published, a new file should be created and should overwrite the previous file. In this text file, the agenda items should be separated by the numbering system of ‘1.’, ‘2.’, ‘3.’, etc.
  - Granicus/GovTV - The Agenda system shall provide an interface allowing the published agenda (HTML format) to be fed to the GovTV system to allow constituents to access the
  - Agendas and meeting minutes via the BOS online meetings (current and past) site on the County of Orange internet page ([http://ocgov.granicus.com/ViewPublisher.php?view\\_id=6](http://ocgov.granicus.com/ViewPublisher.php?view_id=6)).
2. Utilize SQL Server 2016 R2 backend database, if the solution involves hosting and database administration by the County.
3. Be Web based and browser agnostic.

#### B. Board Agenda system Capabilities

Contractor’s Agenda system shall:

1. For ASR submission:
  - Provide a web interface for County Agencies and Departments to create, edit, and submit an ASR.
  - Allow County Agencies and Departments to configure their intra-departmental workflow for routing, tracking changes, collaboration, and approving ASRs internally, prior to the submission of the ASR to the CEO.
  - Allow other Agency/Department-level configurations.
2. For CEO approval:
  - Allow the CEO’s authorized users to review, edit, and approve ASRs that have been submitted.
  - Allow the CEO to customize its intra-departmental workflow for routing, tracking changes, and approving ASRs internally.
  - Allow CEO to track metrics and generate statistics, including but not limited to, the number of ASRs generated, number of ASRs submitted after major deadlines (such as CEO and COB), and number of ASRs that require modifications after submission.
3. For generation of agendas by COB:
  - Allow the COB to generate agendas, reports, and revision/supplemental agendas for a BOS meeting based on the ASRs that have been approved by the CEO.
4. For COB’s Agenda system minute orders:

- Allow the COB to record summary action minutes (SAMs) and issue minute orders and related documents from each BOS meeting.
5. For system configuration:
- Allow the COB to configure both individual County Agency/Department's workflow as well as County-wide workflow that is common to all County Agencies and Departments. Workflow configuration capabilities shall include ability to add approval levels.
  - Allow for other department and county-wide configurations.

**C. Agenda system Features, Functions, and Capabilities**

Contractor's Agenda system shall address the features, functions, and capabilities described in Appendix I – OC Agenda Business Requirements.

**D. Administration**

Contractor's Agenda system shall:

1. Allow modifications, additions, or deletions to drop down menus.
2. Have Microsoft Active Directory integrated:
  - Single Sign-On (SSO) by leveraging the County's existing Identity and Access Management solution, which relies on Microsoft Active Directory Federation Services (ADFS) for single-sign-on.
  - User and Group based security.

**E. Data Migration**

Contractor shall:

1. Migrate existing Agenda Staff Reports (ASRs) that have been published and are in Word documents and their associated attachments (in various file formats, including Word, Excel, PowerPoint, PDF, text, GIF, and TIFF) to the new solution.
2. Provide a solution that incorporates a search capability for the County to search for these ASRs once they have been published – whether those migrated from the existing system or those created in the proposed system. The search capability shall work as follows:
  - Search by title, key words, ASR number, date of hearing, and subject. Keywords are entered by authorized County staff once County Agencies/Departments submit the ASR. Currently, although the files themselves (ASRs and associated attachments) are stored on file servers, the search criteria and keywords are stored in a SQL Server database. Information on the current file folder and database structures can be found in Appendix 2 - Agenda Database Structure for Data Migration.
  - Search results must be read-only.
  - For each ASR returned from the search, the County must be able to view all associated documents such as exhibits, attachments, etc.

**F. On-line Documentation and Help**

Contractor's Agenda system shall:

1. Provide on-line Webinar Trainings.
2. Provide on-line Frequently Asked Questions (FAQs).
3. Provide on-line How To help.



4. Provide on-line Video Trainings.

**G. Performance**

Contractor's Agenda system shall:

1. Move between records in two (2) seconds or less.
2. Move between screens in two (2) seconds or less.
3. Look up a record in three (3) seconds or less (excluding mass search results).
4. Support 200 users simultaneously.

**H. Support for Mobile Device**

Contractor's Agenda system shall:

1. Support Agenda system functions, features and capabilities that may include viewing published Agenda system and/or submitting and approving Agenda system on mobile devices, including, but not limited to, the following operating systems: Smartphones (Android, IOS, and Windows) and Windows Tablets.
2. Provide SSO support for mobile devices.

**I. Deliverables**

1. Contractor shall provide the following deliverables:
  - Complete Requirements and Design for Implementation
  - Complete Software Implementation: Installation, Configuration, Integration, Data Conversion
  - Complete User Acceptance Testing
  - Complete User Training (Software Training, Manuals, and Documentation)
2. Contractor shall provide the following recurring deliverables throughout the term of the Contract:
  - Provide technical support via telephone or remote access 24/7 with a maximum response time of four (4) hours
  - Provide routine patches and Software Updates within one (1) day of their availability

**J. Testing and Acceptance**

Contractor shall:

Facilitate acceptance testing and perform system stress tests of the Agenda system using an agreed upon test script prior to production implementation of the Agenda system as well as through the duration of the Contract, including such times as when major application or module Updates or Upgrades are introduced into the Agenda system.

**K. Training**

Contractor shall:

1. Provide County staff with comprehensive onsite, hands-on training and instruction material to an estimated seventy-five (75) County end users on how to administer and use Contractor's proposed Agenda system.
2. Provide several training methods and curriculums to meet the various roles of County staff. These roles include, but may not be limited to, general users, COB Administrator, County Agency/Department Administrator, Author and Co-Author, County Agency/Department Approver, and CEO Approver.

3. Provide training for County staff in a “Train-the-Trainer” model so the County may assume responsibility for the training of its staff.
4. Provide instructional videos and written training materials for all training applications.
5. Provide training options in technical and specialist areas such as system administration, creating templates and workflows, etc.
6. Conduct training sessions via live webinar format.
7. Provide options for Contractor’s continuous user training on newly released product features and functionality per the training methods listed above.

**L. Implementation**

Contractor shall:

1. Be on-site, with the County, during the Implementation phase, on six (6) separate occasions for a minimum of 3 days for each occasion. This is based on the initial project estimates and may be subject to change depending on implementation plan adjustments of which to be agreed upon between Contractor and County.
2. Schedule: Provide an implementation plan and schedule pursuant to Attachment D – Implementation Plan and Acceptance and Testing Procedures, that provides details of the Deliverables, tasks, activities and associated dates. This plan shall describe the what, when, how, who, and where to implement the Agenda system for the County.
3. Status Reports: Periodically during the Term of this Contract, but not less frequently than once each month, the Contractor shall be responsible for identifying, analyzing, managing and recording issues and risks throughout the Implementation period and will provide the County with an action plan for resolution pursuant to provision 41 “Relationship Management”.
4. Status Meeting: During the Term, representatives of the Parties shall meet and/or teleconference periodically as requested by the County to discuss matters arising under this Contract pursuant to paragraph 40, Relationship Management.

*The rest of this page intentionally left blank*

## Attachment B – Cost Compensation

### I. COMPENSATION

This is a Fixed Fee Schedule Payment Contract between the County and the Contractor for an Agenda system described in Attachment A – Scope of Work, to be provided to the County of Orange.

The Contractor agrees to accept the compensation as set forth in this Attachment B as full remuneration for (a) performing all Services and furnishing all staffing and materials required, (b) any reasonably unforeseen difficulties which may arise or be encountered in the performance of the Services until acceptance, (c) risks connected with the Services, and (d) performance by the Contractor of all its duties and obligations required herein. The County shall have no obligation to pay any sum in excess of the total Contract amount specified herein unless authorized by written amendment.

#### Contractor's Expense

The Contractor will be responsible for all costs related to photocopying, telephone communications, fax communications, travel, parking, and any and all "out of pocket" expenses incurred by the Contractor during the performance of the Services under this Contract, unless otherwise specified. The Contractor shall be responsible for payment of all parking costs and expenses incurred at a County facility while performing work under this Contract, except to the extent the County facility has free parking available to the public and the Contractor makes appropriate use of this free parking. However, the County will at no point provide free parking to the Contractor in the County Civic Center.

### II. PRICING

TABLE I

<b>Implementation Services Milestone Payment Schedule</b>				
<b>Milestone #</b>	<b>Milestone Deliverable</b>	<b>Description</b>	<b>Invoice Amount</b>	<b>Invoice Date</b>
1	Implementation Preparation	Complete Requirements and Design for implementation	20% of One-Time fees - <b>\$10,400</b>	Completion of Milestone
2	Software Implementation	Complete Software Implementation: Installation, Configuration, Integration, Data Conversion	30% of One-Time fees - <b>\$15,600</b>	Completion of Milestone
3	Testing	Complete User Acceptance Testing	20% of One-Time fees - <b>\$10,400</b>	Completion of Milestone
4	Training	Complete User Training (Software Training, Manuals, and Documentation)	20% of One-Time fees - <b>\$10,400</b>	Completion of Milestone

5	Go Live	Software System Ready to Go Live	10% of One-Time fees - \$5,200	Completion of Milestone
<b>Total</b>			<b>\$52,000</b>	

**TABLE II**

Recurring Fees						
ITEM	DESCRIPTION	YEAR 1 (MONTHS 0 – 12)	YEAR 2 (MONTHS 13 – 24)	YEAR 3 (MONTHS 25 – 36)	OPTIONAL YEARS	
					YEARS 4 & 5 (MONTHS 37 – 60)	YEAR 6 & 7 (MONTHS 61 – 72)
1	ANNUAL UNLIMITED SOFTWARE SUBSCRIPTION & MAINTENANCE FEE	\$60,000	\$60,000	\$60,000	\$125,400	\$129,162
	<b>TOTAL ANNUAL RECURRING FEES</b>	<b>\$60,000<sup>1</sup></b>	<b>\$60,000</b>	<b>\$60,000</b>	<b>\$125,400</b>	<b>\$129,162</b>
<b>1</b>	<b>YEAR 1 RECURRING FEE TO BE INVOICED AT CONTRACT EXECUTION.</b>					

**TABLE III**

CONTRACT TOTALS BY YEAR						
	YEAR 1 (MONTHS 0 – 12)	YEAR 2 (MONTHS 13 – 24)	YEAR 3 (MONTHS 25 – 36)	OPTIONAL YEARS		
				YEAR 4 & 5 (MONTHS 37 – 60)	YEAR 6 & 7 (MONTHS 61 – 72)	
<b>ONE-TIME FEES (TABLE I)</b>	\$52,000	N/A	N/A	N/A	N/A	
<b>RECURRING FEES (TABLE II)</b>	\$60,000	\$60,000	\$60,000	\$125,400	\$129,162	
<b>YEAR(S) TOTAL</b>	<b>\$112,000</b>	<b>\$60,000</b>	<b>\$60,000</b>	<b>\$125,400</b>	<b>\$129,162</b>	
<b>CONTINGENCY AMOUNT –</b>	<b>\$10,000</b>					
		<b>3 YEAR TOTAL (40 MONTHS)</b>	<b>\$220,000</b>	<b>7 YEAR TOTAL (88 MONTHS)</b>	<b>\$486,562<sup>1</sup></b>	
<b>1</b>	<b>7 YEAR TOTAL INCLUDES \$10,000 CONTINGENCY AMOUNT</b>					

**TABLE IV**

PRIME GOVERNMENT SOLUTIONS HOURLY RATE FOR SERVICES OUTSIDE OF THE SCOPE OF WORK
<b>\$200 PER HOUR</b>

**III. FEE REDUCTIONS**

Fee Reductions for missed performance have been designed to encourage the consistent and timely delivery of service and value to the County. The Fee Reductions are not intended to compensate the County for damages, but rather to reimburse the County for the value of the diminished services actually delivered, and to provide incentive to the Contractor to achieve the Contract's stated objectives and focus on the County's critical needs.

The Fee Reduction tables included below outline the circumstances under which the County will be entitled to Fee Reductions for Contractor's failure to meet the Contract "Go-Live" date or achieve the Service Level Requirements.

**A. Service Level Requirements, Performance Thresholds, and Fee Reduction Amounts**

**Table 1 – Solution Availability**

Measurement for Solution Availability is defined as the percentage of time the Solution is fully operational and available when called upon during a calendar month. Availability represents a measure of the fraction of time (expressed as a percentage) during a defined period when the Service or System is deemed to be equal to or better than a designated Service Level.

$$\text{Solution Availability \%} = \frac{\text{Scheduled Uptime} - \text{Scheduled Downtime}}{\text{Scheduled Uptime} + \text{Unplanned Outage}}$$

<b>Service Level Requirement</b>	<b>Performance Threshold (monthly)</b>	<b>Service Credit Amount</b>
Solution Availability	>= 99.96% Availability	No reduction
Solution Availability	< = 99.95% Availability	1% of All Annual Charges
Solution Availability	< = 95.00% Availability	10% of All Annual Charges
Solution Availability	< = 90.00% Availability	25% of All Annual Charges

**B. Applying Fee Reductions**

Service Credits based on Solution Availability shall be applied to the following annual maintenance recurring fee invoice. In the event there are no following invoices, the Contractor shall issue a check in the amount of the Service Credit payable to the County.

**IV. PAYMENT TERMS**

The Contractor shall reference the Contract number on the invoice. Payment shall be net forty-five (45) days after receipt of an invoice in a format acceptable to the County and verified and approved by the agency/department and subject to routine processing requirements.

Billing shall cover Services and/or goods not previously invoiced. The Contractor shall reimburse the County for any monies paid to the Contractor for goods or Services not provided or when goods or Services do not meet the Contract requirements.

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

**V. PAYMENT/INVOICING INSTRUCTIONS**

The Contractor shall provide an invoice on the Contractor's letterhead for Services rendered. Each invoice shall have a number and shall include the following information:

1. Contractor's name and address;

2. Contractor's remittance address (if different from 1 above);
3. Name of County agency or department;
4. County Contract number;
5. Service Date(s);
6. Service Description;
7. Cost;
8. Contractor's Federal I. D. number; and
9. Total.

The responsibility for providing an acceptable invoice to the County for payment rests with the Contractor. Incomplete or incorrect invoices are not acceptable and shall be returned to the Contractor for correction. The County's Project Manager, or designee, is responsible for approval of invoices and subsequent submittal of invoices to OCIT Accounts Payable for processing of payment.

Invoices and support documentation are to be forwarded to:

County of Orange  
Information Technology  
Attn: Accounts Payable  
1055 N. Maint St.  
6th Floor  
Santa Ana, CA 92701

*The rest of this page intentionally left blank*

**Attachment C – Staffing Plan**

**Contractor staffing team to perform the requirements set forth in the Contract’s Attachment A, Scope of Work.**

<b>Name and Title</b>	<b>Role in Project</b>
Sherif Agib	Executive Stakeholder
Padraig Supple	Project Manager
Larry Thorpe	Technical Team Lead
Spencer Bigler	Business Analyst

*The rest of this page intentionally left blank*

**Attachment D – Implementation Plan, Acceptance, and Testing Procedures**

**Contractor will provide an Implementation Plan and Acceptance and Testing Procedures to be used to ensure Services are provided in compliance with County specifications and requirements, including, but not limited to, the following:**

- a. The Implementation Plan shall include but not be limited to: Onboarding Assessment, Gap Analysis, Pre-Implementation Planning, Data Conversion, Development, Integrations, Training, User Acceptance, Go Live, Support, and Roadmap. See Appendix I, OC Agenda Business Requirements and Roadmap, for detailed product features and task along with their corresponding development dates.
- b. The Contractor shall deliver Software(s) with the appropriate configurations to support the County's requirements at the end of the implementation phase, as specified in the Contract.
- c. The Contractor shall provide professional services to implement the proposed Agenda system (includes project management, solution and report development, data conversion, and testing).
- d. Software configurations, functional and non-functional system testing, data conversion, report development and testing, system integration testing and user acceptance testing are all part of the Contractor's implementation plan.
- e. The Contractor shall integrate the proposed Agenda system with other County systems or provide data feed to these systems, including the Crestron system and GovTV, based on mutually agreed interface requirements and/or business processes specified herein. Integration must be through industry standard interfaces.

*The rest of this page intentionally left blank*



**Attachment E – Annual Maintenance and Support**

**Contractor shall provide Annual Maintenance and Support that, at a minimum, meet the following requirements:**

- a. The Contractor shall provide all Agenda system Software maintenance and warranty Updates, Upgrades, patches, fixes, etc. at no additional cost.
- b. The Contractor's Software maintenance and warranty services will extend to all configurations, workflow development, and report development efforts included in the solution implementation.
- c. The Contractor shall provide response times based on the priority levels of issues reported by the customer as per this contract and Attachment J – Prime Government Solutions Service Level Agreement. Resolution times will be provided with reasonable estimations based on severity and impact to customer and in accordance with Attachment J – Prime Government Solutions Service Level Agreement.
- d. The Contractor shall use commercially reasonable efforts to provide modifications or Upgrades to the Software to retain compatibility with future Microsoft Office products.
- e. On-Call Support - During the term of the Contract, the Contractor shall provide phone/online support to identify and correct bugs between releases between 6 am through 6 pm PT, Monday through Sunday.

*The rest of this page intentionally left blank*

**Attachment F – Solution Delivery Hosted/Managed**

**I. The Contractor shall be responsible for end-to-end, secure hosting and technical support of all Hardware and Software required to operate the Contractor’s proposed solution. The Contractor’s Infrastructure Management Services shall include:**

**1. Hosting**

- 1.1 The Contractor’s solution shall be hosted in a highly secure data center located in the United States and no information shall cross country borders. The solution shall have sufficient Internet bandwidth, computing capacity, security, storage, monitoring, disaster recovery and IT service management and incident response processes to meet County technical requirements, security requirements and solution performance metrics.
- 1.2 The Contractor will implement and maintain a disaster recovery plan that provides for the continued delivery of the Service in the event of a power outage, system outage or other circumstances that may interrupt the normal provision of the Service.
- 1.3 The Contractor shall cooperate with any County on-site audit or penetration test of Contractor managed systems.
- 1.4 Annually, the Contractor shall provide the SOC 1 Type I or Type II Report.

**2. Architectural, Performance, Sizing and Capacity Planning**

- 2.1 The Contractor shall provide system architectural, sizing and capacity planning recommendations that will enable the production Agenda System to operate at optimal performance and within acceptable County Service Levels at all times.
- 2.2 The Contractor shall provide a solution that meets County performance, security and infrastructure requirements.
- 2.3 The Contractor shall conduct routine architectural, capacity and operational reviews of the County’s production solution environment and, at a minimum, annually implement architectural improvements to improve solution performance, availability, reliability and sustainability in accordance with County Service Levels.

**3. IT Service Management**

- 3.1 The Contractor shall manage the solution and all supporting software and hardware within the Contractor’s hosted environment under a consistent set of IT life cycle service management framework that utilizes industry standards and best practices.
- 3.2 The Contractor shall perform system changes in accordance with an agreed upon change management and notification process.
- 3.3 The Contractor shall perform routine system maintenance, including OS patching, critical and high security Updates and patching, and planned System changes for Contractor’s hosted environment and managed hardware provided to the County, within an agreed upon maintenance window or County agreed upon schedule.
- 3.4 The Contractor shall perform industry standard data backup plans for daily, weekly and monthly backups. The Contractor shall use backups to restore data in the event of an outage or Incident.

**4 Application Performance Testing, Monitoring and Reporting**

- 4.2 To ensure the County Agenda system performs at desired levels, the Contractor shall be required to test, monitor and report on the System performance activity. The Contractor shall monitor the County's experience to ensure that the application and its interfaces are performing within County defined service level requirements.
- 4.3 The Contractor shall document the service level requirements issues and notify County contacts via e-mail when service levels are below acceptable levels.
- 4.4 The Contractor shall identify the root cause of performance degradation and take corrective action to resolve issues and promptly bring service level back within acceptable levels.
- 4.5 The Contractor shall provide monthly service level reports that demonstrate compliance according to Attachment J – Prime Government Solutions Service Level Agreement.

## **5 Security**

- 5.2 All Contractor -hosted infrastructure shall be secured in a manner acceptable to the County in accordance with standard industry security compliances and best practices.
- 5.3 The Contractor's solution will integrate with the County's Active Directory System using Security Assertion Markup Language (SAML) for single sign-on. This authentication methodology will be available before the Go Live date.
- 5.4 The Contractor's solution will allow County users to access the Application via the Internet using HTTPS and support multi-factor authentication (MFA).
- 5.5 Any passwords required by the Contractor's solution shall be securely stored with a minimum of 256-bit encryption, a cryptographic hash function, or other technology as will be made available in the future, and in accordance with County best business practice for passwords.
- 5.6 The Contractor's solution shall transmit data using a secure transaction.
- 5.7 The Contractor's solution sessions shall support the latest Transport Layer Security (TLS) version that is supported by the parties. The TLS version used must be consistent with the ability to provide access to County systems. This means the service must utilize the same TLS version as the County computer systems.
- 5.8 The Contractor's solution will require no thick client piece to be installed or supported at the host level, and all access to the application will be through a web browser.
- 5.9 The Contractor's solution shall have a unique account for each end user that supports strong, non-repudiation with audit capabilities.
- 5.10 The Contractor shall have independent third-party security audits performed annually and a copy of the report shall be provided to the County upon request. Reports from any additional security audits shall also be provided to the County upon request.
- 5.11 The Contractor shall comply with all state and federal statutes and regulations concerning the privacy and confidentiality of information (GLB, HIPAA, AB1386, etc.), if applicable to this Contract, including those statutes and regulations set forth in the Contract.
- 5.12 Upon County request, the Contractor shall provide the County a copy of their System Reuse and Mass Storage Decommissioning Policies.
- 5.13 The Contractor shall immediately notify the County of any and all intrusions, security violations and/or Incidents. The County reserves the right to participate in any consequential investigation at the level of involvement deemed necessary by the County.

5.14 The above requirements will be reviewed by the County and the Contractor annually on the anniversary of contract award or more frequently as reasonably determined by the County to reflect changes in best practices and technology.

## **6 Performance Guarantees**

6.2 The Contractor shall incur fee reductions for failing to successfully maintain Service Performance Guarantees as set forth in Attachment B and Attachment J. The County reserves the right to allocate the percentage of the fee reductions for each performance guarantee with no more than 20% allocated to any one performance standard. Additionally, the County requires the ability to re-allocate the fee reductions amount for each performance standard annually.

6.3 The Contractor agrees that member satisfaction and account satisfaction shall be measured and reported to the County within forty-five (45) business days of each calendar year. All other service performance guarantees shall be measured and reported directly to the County by the tenth (10th) business day of the following month.

6.4 When performance issues are identified, the Contractor will agree to provide a corrective action plan within seventy-two (72) hours of identification of the issue. Once agreed to by the County, the actions and timelines will be adhered to.

6.5 The Contractor agrees that all reporting provided to the County will include the County's aggregated plan experience unless the County requests reporting to be segregated by business unit or plan.

## **II. Data Ownership**

1. The County will solely own the Agenda system's data.
2. The Contractor shall safeguard the County's data from co-mingling with data of various Contractor customers.
3. The Contractor shall return data upon termination of the Contract or upon demand. The Contractor shall destroy County's data once the County has verified that all County data has been returned.
4. The Contractor shall recover data in the event of System failure.

*The rest of this page intentionally left blank*

**Attachment G – Business Associate Contract**

**(See separate Attachment titled “Business Associate Contract County of Orange”)**

**Attachment H – Information Technology Security Policy**  
**County of Orange**

**(See separate Attachment entitled “Information Technology Security Policy County of Orange”)**

**Attachment I – Prime Government Solutions Service Agreement**

**(See separate attachment entitled “Prime Government Solutions Service Agreement”)**

**Attachment J – Prime Government Solutions Service Level Agreement**

**(See separate attachment entitled “Prime Government Solutions Service Level Agreement”)**



**Attachment K – Prime Government Solutions Security Policies and Procedures**

**(See separate attachment entitled “Prime Government Solutions Security Policies and Procedures”)**

**Appendix 1: OC Agenda Business Requirements and Roadmap**

**(See separate attachment entitled “OC Agenda Business Requirements and Roadmap”)**

**Appendix 2: Agenda Database Structure for Data Migration**

**(See separate attachment entitled “Agenda Database Structure for Data Migration”)**

**Appendix 3: Sample Feed to Crestron**

**(See separate attachment entitled “Sample Feed to Crestron”)**

**ATTACHMENT G**  
**BUSINESS ASSOCIATE CONTRACT**

**A. GENERAL PROVISIONS AND RECITALS**

1. The Parties agree that the terms used, but not otherwise defined below in Paragraph B, shall have the same meaning given to such terms under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (DHHS) ("the HIPAA regulations") (45 CFR Parts 160, 162 and 164) as they may exist now or be hereafter amended.

2. The Parties agree that a business associate relationship under HIPAA, the HITECH Act, and the HIPAA regulations between the Contractor and County arises to the extent that Contractor performs, or delegates to subcontractors to perform, functions or activities on behalf of County pursuant to, and as set forth in, the Agreement that are described in the definition of "Business Associate" in 45 CFR § 160.103.

3. The County wishes to disclose to Contractor certain information pursuant to the terms of the Agreement, some of which may constitute Protected Health Information ("PHI"), as defined below in Subparagraph B.10, to be used or disclosed in the course of providing services and activities pursuant to, and as set forth, in the Agreement.

4. The Parties intend to protect the privacy and provide for the security of PHI that may be created, received, maintained, transmitted, used, or disclosed pursuant to the Agreement in compliance with the applicable standards, implementation specifications, and requirements of HIPAA, the HITECH Act, and the HIPAA regulations as they may exist now or be hereafter amended.

5. The Parties understand and acknowledge that HIPAA, the HITECH Act, and the HIPAA regulations do not pre-empt any state statutes, rules, or regulations that are not otherwise pre-empted by other Federal law(s) and impose more stringent requirements with respect to privacy of PHI.

6. The Parties understand that the HIPAA Privacy and Security rules, as defined below in Subparagraphs B.9 and B.14, apply to the Contractor in the same manner as they apply to a covered entity (County). Contractor agrees therefore to be in compliance at all times with the terms of this Business Associate Contract and the applicable standards, implementation specifications, and requirements of the Privacy and the Security rules, as they may exist now or be hereafter amended, with respect to PHI and electronic PHI created, received, maintained, transmitted, used, or disclosed pursuant to the Agreement.

**B. DEFINITIONS**

1. "Administrative Safeguards" are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect

electronic PHI and to manage the conduct of Contractor's workforce in relation to the protection of that information.

2. "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

a. Breach excludes:

i. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of Contractor or County, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

ii. Any inadvertent disclosure by a person who is authorized to access PHI at Contractor to another person authorized to access PHI at the Contractor, or organized health care arrangement in which County participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.

iii. A disclosure of PHI where Contractor or County has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

b. Except as provided in paragraph (a) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless Contractor demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

ii. The unauthorized person who used the PHI or to whom the disclosure was made;

iii. Whether the PHI was actually acquired or viewed; and

iv. The extent to which the risk to the PHI has been mitigated.

3. "Data Aggregation" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.

4. "Designated Record Set" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.

5. "Disclosure" shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.

6. "Health Care Operations" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.

7. "Individual" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

8. "Physical Safeguards" are physical measures, policies, and procedures to protect

CONTRACTOR's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

9. "The HIPAA Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

10. "Protected Health Information" or "PHI" shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.

11. "Required by Law" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.103.

12. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

13. "Security Incident" means attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. "Security incident" does not include trivial incidents that occur on a daily basis, such as scans, "pings", or unsuccessful attempts to penetrate computer networks or servers maintained by Contractor.

14. "The HIPAA Security Rule" shall mean the Security Standards for the Protection of electronic PHI at 45 CFR Part 160, Part 162, and Part 164, Subparts A and C.

15. "Subcontractor" shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.

16. "Technical safeguards" means the technology and the policy and procedures for its use that protect electronic PHI and control access to it.

17. "Unsecured PHI" or "PHI that is unsecured" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued on the HHS Web site –

<http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html> .

18. "Use" shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.

C. OBLIGATIONS AND ACTIVITIES OF CONTRACTOR AS BUSINESS ASSOCIATE:

1. Contractor agrees not to use or further disclose PHI County discloses to Contractor other than as permitted or required by this Business Associate Contract or as required by law.

2. Contractor agrees to use appropriate safeguards, as provided for in this Business Associate Contract and the **Agreement**, to prevent use or disclosure of PHI County discloses to Contractor or Contractor creates, receives, maintains, or transmits on behalf of County other than as provided for by this Business Associate Contract.

3. Contractor agrees to comply with the HIPAA Security Rule at Subpart C of 45 CFR Part 164 with respect to electronic PHI County discloses to Contractor or Contractor creates, receives,

maintains, or transmits on behalf of County.

4. Contractor agrees to mitigate, to the extent practicable, any harmful effect that is known to Contractor of a Use or Disclosure of PHI by Contractor in violation of the requirements of this Business Associate Contract.

5. Contractor agrees to report to County immediately any Use or Disclosure of PHI not provided for by this Business Associate Contract of which Contractor becomes aware. Contractor must report Breaches of Unsecured PHI in accordance with Paragraph E below and as required by 45 CFR § 164.410.

6. Contractor agrees to ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of Contractor agree to the same restrictions and conditions that apply through this Business Associate Contract to Contractor with respect to such information.

7. Contractor agrees to provide access, within fifteen (15) calendar days of receipt of a written request by County, to PHI in a Designated Record Set, to County or, as directed by County, to an Individual in order to meet the requirements under 45 CFR § 164.524.

8. Contractor agrees to make any amendment(s) to PHI in a Designated Record Set that County directs or agrees to pursuant to 45 CFR § 164.526 at the request of County or an Individual, within thirty (30) calendar days of receipt of said request by County. Contractor agrees to notify County in writing no later than ten (10) calendar days after said amendment is completed.

9. Contractor agrees to make internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by Contractor on behalf of, County available to County and the Secretary in a time and manner as determined by County or as designated by the Secretary for purposes of the Secretary determining County's compliance with the HIPAA Privacy Rule.

10. Contractor agrees to document any Disclosures of PHI County discloses to Contractor or Contractor creates, receives, maintains, or transmits on behalf of County, and to make information related to such Disclosures available as would be required for County to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR § 164.528.

11. Contractor agrees to provide County or an Individual, as directed by County, in a time and manner to be determined by County, that information collected in accordance with the **Agreement**, in order to permit County to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR § 164.528.

12. Contractor agrees that to the extent Contractor carries out County's obligation under the HIPAA Privacy and/or Security rules Contractor will comply with the requirements of 45 CFR Part 164 that apply to County in the performance of such obligation.

13. Contractor shall work with County upon notification by Contractor to County of a Breach to properly determine if any Breach exclusions exist as defined in Subparagraph B.2.a above.



D. SECURITY RULE

1. Contractor shall comply with the requirements of 45 CFR § 164.306 and establish and maintain appropriate Administrative, Physical and Technical Safeguards in accordance with 45 CFR § 164.308, § 164.310, § 164.312, and § 164.316 with respect to electronic PHI County discloses to Contractor or Contractor creates, receives, maintains, or transmits on behalf of County. Contractor shall follow generally accepted system security principles and the requirements of the HIPAA Security Rule pertaining to the security of electronic PHI.

2. Contractor shall ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of Contractor agree through a contract with Contractor to the same restrictions and requirements contained in this Paragraph D of this Business Associate Contract.

3. Contractor shall report to County immediately any Security Incident of which it becomes aware. Contractor shall report Breaches of Unsecured PHI in accordance with Paragraph E below and as required by 45 CFR § 164.410.

E. BREACH DISCOVERY AND NOTIFICATION

1. Following the discovery of a Breach of Unsecured PHI , Contractor shall notify County of such Breach, however both Parties agree to a delay in the notification if so advised by a law enforcement official pursuant to 45 CFR § 164.412.

a. A Breach shall be treated as discovered by Contractor as of the first day on which such Breach is known to Contractor or, by exercising reasonable diligence, would have been known to Contractor.

b. Contractor shall be deemed to have knowledge of a Breach, if the Breach is known, or by exercising reasonable diligence would have known, to any person who is an employee, officer, or other agent of Contractor, as determined by federal common law of agency.

2. Contractor shall provide the notification of the Breach immediately to the County Privacy Officer at:

Linda Le, Interim Chief Information Security Officer, CHPC, CHC, CHP OCIT – Enterprise Security 1501 E. St. Andrews Place Santa Ana, CA 92705 (714) 834-4082 <a href="mailto:Linda.Le@ceoit.ocgov.com">Linda.Le@ceoit.ocgov.com</a>	Linda Le, County Privacy Officer, CHPC, CHC, CHP OCIT – Enterprise Security 1501 E. St. Andrews Place Santa Ana, CA 92705 (714) 834-4082 <a href="mailto:Linda.le@ceoit.ocgov.com">Linda.le@ceoit.ocgov.com</a> <a href="mailto:privacyofficer@ocgov.com">privacyofficer@ocgov.com</a>
--	--

a. Contractor's notification may be oral, but shall be followed by written notification within 24 hours of the oral notification.

3. Contractor's notification shall include, to the extent possible:

a. The identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Contractor to have been, accessed, acquired, used, or disclosed during the Breach;

b. Any other information that County is required to include in the notification to Individual under 45 CFR §164.404 (c) at the time Contractor is required to notify County or promptly thereafter as this information becomes available, even after the regulatory sixty (60) day period set forth in 45 CFR § 164.410 (b) has elapsed, including:

(1) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

(2) A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(3) Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;

(4) A brief description of what Contractor is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any future Breaches; and

(5) Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

4. County may require Contractor to provide notice to the Individual as required in 45 CFR § 164.404, if it is reasonable to do so under the circumstances, at the sole discretion of the County.

5. In the event that Contractor is responsible for a Breach of Unsecured PHI in violation of the HIPAA Privacy Rule, Contractor shall have the burden of demonstrating that Contractor made all notifications to County consistent with this Paragraph E and as required by the Breach notification regulations, or, in the alternative, that the acquisition, access, use, or disclosure of PHI did not constitute a Breach.

6. Contractor shall maintain documentation of all required notifications of a Breach or its risk assessment under 45 CFR § 164.402 to demonstrate that a Breach did not occur.

7. Contractor shall provide to County all specific and pertinent information about the Breach, including the information listed in Section E.3.b.(1)-(5) above, if not yet provided, to permit County to meet its notification obligations under Subpart D of 45 CFR Part 164 as soon as practicable, but in no event later than fifteen (15) calendar days after Contractor's initial report of the Breach to County pursuant to Subparagraph E.2 above.

8. Contractor shall continue to provide all additional pertinent information about the Breach to

County as it may become available, in reporting increments of five (5) business days after the last report to County. Contractor shall also respond in good faith to any reasonable requests for further information, or follow-up information after report to County, when such request is made by County.

9. Contractor shall bear all expense or other costs associated with the Breach and shall reimburse County for all expenses County incurs in addressing the Breach and consequences thereof, including costs of investigation, notification, remediation, documentation or other costs associated with addressing the Breach.

#### F. PERMITTED USES AND DISCLOSURES BY CONTRACTOR

1. Contractor may use or further disclose PHI County discloses to Contractor as necessary to perform functions, activities, or services for, or on behalf of, County as specified in the Agreement, provided that such use or Disclosure would not violate the HIPAA Privacy Rule if done by COUNTY except for the specific Uses and Disclosures set forth below.

a. Contractor may use PHI County discloses to Contractor, if necessary, for the proper management and administration of Contractor.

b. Contractor may disclose PHI County discloses to Contractor for the proper management and administration of Contractor or to carry out the legal responsibilities of Contractor, if:

i. The Disclosure is required by law; or

ii. Contractor obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person and the person immediately notifies Contractor of any instance of which it is aware in which the confidentiality of the information has been breached.

c. Contractor may use or further disclose PHI County discloses to Contractor to provide Data Aggregation services relating to the Health Care Operations of Contractor.

2. Contractor may use PHI County discloses to Contractor, if necessary, to carry out legal responsibilities of Contractor.

3. Contractor may use and disclose PHI County discloses to Contractor consistent with the minimum necessary policies and procedures of County.

4. Contractor may use or disclose PHI County discloses to Contractor as required by law.

#### G. OBLIGATIONS OF COUNTY

1. County shall notify Contractor of any limitation(s) in County's notice of privacy practices in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Contractor's Use or Disclosure of PHI.

2. County shall notify Contractor of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect Contractor's Use

or Disclosure of PHI.

3. County shall notify Contractor of any restriction to the Use or Disclosure of PHI that County has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Contractor's Use or Disclosure of PHI.

4. County shall not request Contractor to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule if done by County.

#### H. BUSINESS ASSOCIATE TERMINATION

1. Upon County's knowledge of a material breach or violation by Contractor of the requirements of this Business Associate Contract, County shall:

a. Provide an opportunity for Contractor to cure the material breach or end the violation within thirty (30) business days; or

b. Immediately terminate the Agreement, if Contractor is unwilling or unable to cure the material breach or end the violation within (30) days, provided termination of the Agreement is feasible.

2. Upon termination of the Agreement, Contractor shall either destroy or return to County all PHI Contractor received from County or Contractor created, maintained, or received on behalf of County in conformity with the HIPAA Privacy Rule.

a. This provision shall apply to all PHI that is in the possession of Subcontractors or agents of Contractor.

b. Contractor shall retain no copies of the PHI.

c. In the event that Contractor determines that returning or destroying the PHI is not feasible, Contractor shall provide to County notification of the conditions that make return or destruction infeasible. Upon determination by County that return or destruction of PHI is infeasible, Contractor shall extend the protections of this Business Associate Contract to such PHI and limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction infeasible, for as long as Contractor maintains such PHI.

3. The obligations of this Business Associate Contract shall survive the termination of the Agreement.

**Attachment J – Prime Government Solutions Service Level Agreement**

**SCHEDULE 1 – Support Services SLA**

The SLA describes the expected performance of the PrimeGov Service, the procedures for reporting an issue and expected turnaround time on issues reported.

**A. Service Uptime Target**

PrimeGov have a target uptime of >99.95% measured on a monthly basis. This time excludes any planned outages that have been identified to the Customer. PrimeGov must give a minimum of two business days notice for a planned outage. Planned outages will be targeted to occur between 00:01 on Saturdays to 23:59 on Sunday night.

**B. Reporting an Issue**

**1. Contact Details**

At PrimeGov we build our Service with alerting to anticipate any Service disruption so that our Customer Success team can address any technical items before they become an issue for our customers. In the case where a Customer discovers a defect or fault, or the Service is unavailable, the Customer should notify the PrimeGov Customer Success team through one of the following channels:

- Enter a ticket in the help desk system at [primegov.freshdesk.com](http://primegov.freshdesk.com)
- E-mail: [support@primegov.com](mailto:support@primegov.com)
- Phone: 801-341-1910

**2. Hours of Coverage**

The Support Services will be provided between Business Days 08:00 to 18.00 MT, from Monday to Friday. More specifically, the hours are as follows:

- Service support 08:00 to 18.00 MT
- Enter an issue in the help desk system This service will be available 24 hours a day – 7 days a week
- Email an issue to the Customer Success team This service will be available 24 hours a day – 7 days a week

**3. Customer Priority Identification**

The Customer will supply their determined priority for each support item logged in accordance with the following Priority Code.

Priority Code	Description
P1	<b>Critical</b> - The problem is impacting all Users by the Service being unavailable with no work around available.
P2	<b>High</b> - The problem is impacting a significant number of Users and is causing a significant business impact, where there is no workaround available.
P3	<b>Moderate</b> - The problem is impacting a small number of Users and is causing a minor business impact or is causing a significant business impact, but there is a workaround available
P4	<b>Low</b> – NON-SERVICE AFFECTING DEFECT –Non-urgent or cosmetic problems, queries, causing inconvenience only.

**C. Resolving an Issue**

**1. Steps to Resolution**

- a) PrimeGov Customer Success staff will analyze the issue and revert to the Customer with an assessment of the issue
- b) The issue will then result in one of the following actions:
  - a. The PrimeGov Customer Success staff will send a set of steps to close the issue with associated times.
  - b. PrimeGov Customer Success staff will ask for more clarification/ information on the issue.
  - c. PrimeGov Customer Success staff may discuss the priority of the issue.
- c) The Customer and the PrimeGov Customer Success staff will mutually agree to close or reprioritize an issue.
- d) If a support issue is closed because it has been successfully resolved, then PrimeGov Customer Success staff will provide a brief description of the final solution to the Customer.
- e) If a support issue is closed but it has not been successfully resolved, then PrimeGov Customer Success staff will provide a brief description of the reason for closing the issue to the Customer.

**2. Target Response Time**

PrimeGov will aim to provide the Customer with a response within a specific time limit based on the agreed Priority Code of the Support Issue (a "Target Response Time"). The following Target Response Times are within the Hours of Coverage.

Priority Code	Description	Target Response Time <	Target Resolution Time <
P1	Critical	30 Minutes	4 Hours
P2	High	1 Hour	16 Hours
P3	Moderate	2 Hours	80 Hours
P4	Low	40 Hours	Future Planned Release

**3. Problem Escalation**

A Support Call's Priority Code may be escalated by either the Customer or PrimeGov, if it is found to be more business critical than first realized or if the steps to resolve are proving unsatisfactory. In the event of escalation the following contacts from PrimeGov should be called:

Role	Name	Contact Details
V.P. Customer Success	Luis Martinez	luis.martinez@primegov.com
Director	XXX	XXX
CEO	Rich Drew	rich.drew@primegov.com

**4. Minor Enhancements**

Requests by the Customer for minor enhancements or changes to the Service not relating to a defect or error inherent in the Service will be considered on a case by case basis and will be included under this Agreement at the sole discretion of PrimeGov if in the PrimeGov software product roadmap.

**5. Exclusions**

- a) Requests by the Customer for significant enhancements or changes to the Service not relating to a defect or error inherent in the Service will be excluded from this Agreement and will be managed separately.
- b) PrimeGov is only obliged to provide the Support Services with respect to the then current version of the Service. If PrimeGov provides Support Services for older versions/releases, this is done without obligation on an "as-is" basis at PrimeGov's sole discretion and without any service level applying and PrimeGov may make the provision of further Support Services for older versions of the Service subject to the payment of additional fees.
- c) any alteration, modification or maintenance of the Service by the Customer or any third party which has not been authorized in writing by PrimeGov;
- d) any failure by the Customer to implement any recommendations, solutions to faults, problems or updates previously advised or delivered by PrimeGov to the Customer;
- e) either Party being subject to Force Majeure;
- f) the Customer's failure, inability or refusal to allow PrimeGov's personnel proper and uninterrupted access to the Service;



---

Prime Government Solutions | 220 N. 1200 E. #201 Lehi, UT 84043 | 801-341-1910 | info@primegov.com

# Policy Documentation

## Contents

Email Policy .....	2
Acceptable Use Policy .....	4
Password Protection Policy .....	8
Password Construction Guidelines .....	10
Data Protection Policy .....	11
Remote Access Policy.....	13
Server Security Policy.....	15
Security Response Plan Policy.....	17

# Email Policy

## Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

## Purpose

The purpose of this email policy is to ensure the proper use of the PrimeGov email system and make users aware of what PrimeGov deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within the PrimeGov Network.

## Scope

This policy covers appropriate use of any email sent from a PrimeGov email address and applies to all employees, vendors, and agents operating on behalf of PrimeGov.

## Policy

1. All use of email must be consistent with PrimeGov policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
2. PrimeGov email account should be used primarily for PrimeGov business-related purposes; personal communication is permitted on a limited basis, but non-PrimeGov related commercial uses are prohibited.
3. All PrimeGov data contained within an email message or an attachment must be secured according to the *Password Construction Guidelines*

## Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network. This guideline provides best practices for creating secure passwords.

## Purpose

The purpose of this guidelines is to provide best practices for the creation of strong passwords.

## Scope

This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

## Policy

### Statement of Guidelines

Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include "It's time for vacation" or "block-curious-sunny-leaves". Passphrases are both easy to remember and type, yet meet the strength requirements.

Poor, or weak, passwords have the following characteristics:

- Contain eight characters or less.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Are some version of "Welcome123" "Password123" "Changeme123"

In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of 'password manager' software that is authorized and provided by the organization. Whenever possible, also enable the use of multifactor authentication.



## Policy Compliance

### Compliance Measurement

The policy owner will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

### Exceptions

Any exception to the policy must be approved by the policy owner in advance.

### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

*Password Protection Policy*

## Definitions and Terms

None

4. Data Protection Policy.
5. Email should be retained only if it qualifies as a PrimeGov business record. Email is a PrimeGov business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
6. Email that is identified as a PrimeGov business record shall be retained according to PrimeGov Record Retention Schedule.
7. The PrimeGov email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any PrimeGov employee should report the matter to their supervisor immediately.
8. Users are prohibited from automatically forwarding PrimeGov email to a third-party email system (noted directly below). Individual messages which are forwarded by the user must not contain PrimeGov confidential or above information.
9. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct PrimeGov business, to create or memorialize any binding transactions, or to store or retain email on behalf of PrimeGov. Such communications and transactions should be conducted through proper channels using PrimeGov-approved documentation.
10. Using a reasonable amount of PrimeGov resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a PrimeGov email account is prohibited.
11. PrimeGov employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
12. PrimeGov may monitor messages without prior notice. PrimeGov is not obliged to monitor email messages.

## Policy Compliance

### Compliance Measurement

The Policy owner will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

### Exceptions

Any exception to the policy must be approved by the Policy owner in advance.

### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

### *Password Construction Guidelines*

#### Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network. This guideline provides best practices for creating secure passwords.

#### Purpose

The purpose of this guidelines is to provide best practices for the creation of strong passwords.

#### Scope

This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

#### Policy

##### Statement of Guidelines

Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include "It's time for vacation" or "block-curious-sunny-leaves". Passphrases are both easy to remember and type, yet meet the strength requirements.

Poor, or weak, passwords have the following characteristics:

- Contain eight characters or less.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Are some version of "Welcome123" "Password123" "Changeme123"

In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of 'password manager' software that is authorized and provided by the organization. Whenever possible, also enable the use of multifactor authentication.

#### Policy Compliance

##### Compliance Measurement

The policy owner will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

##### Exceptions

Any exception to the policy must be approved by the policy owner in advance.

##### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

### *Password Protection Policy*

#### Definitions and Terms

None

Data Protection Policy

**Definitions and Terms**

None

# Acceptable Use Policy

## Overview

PrimeGov's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to PrimeGov's established culture of openness, trust and integrity. We are committed to protecting PrimeGov's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of PrimeGov. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every PrimeGov employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

## Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at PrimeGov. These rules are in place to protect the employee and PrimeGov. Inappropriate use exposes PrimeGov to risks including virus attacks, compromise of network systems and services, and legal issues.

## Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct PrimeGov business or interact with internal networks and business systems, whether owned or leased by PrimeGov, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at PrimeGov and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with PrimeGov policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at PrimeGov, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by PrimeGov.

## Policy

### General Use and Ownership

1. PrimeGov proprietary information stored on electronic and computing devices whether owned or leased by PrimeGov, the employee or a third party, remains the sole property of PrimeGov. You must ensure through legal or technical means that proprietary information is protected.
2. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of PrimeGov proprietary information.
3. You may access, use or share PrimeGov proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
5. For security and network maintenance purposes, authorized individuals within PrimeGov may monitor equipment, systems and network traffic at any time.
6. PrimeGov reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

### Security and Proprietary Information

1. All mobile and computing devices that connect to the internal network must comply with this policy.
2. System level and user level passwords must comply with the *Password Protection Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
3. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4. Postings by employees from a PrimeGov email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of PrimeGov, unless posting is in the course of business duties.
5. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

### **Unacceptable Use**

1. The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
2. Under no circumstances is an employee of PrimeGov authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing PrimeGov-owned resources.
3. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

### **System and Network Activities**

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by PrimeGov.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which PrimeGov or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting PrimeGov business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a PrimeGov computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any PrimeGov account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the Policy owner is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, or similar technology on the PrimeGov network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, PrimeGov employees to parties outside PrimeGov.

**Email and Communication Activities**

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the Technical Team Lead.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within PrimeGov's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by PrimeGov or connected via PrimeGov's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

**Blogging and Social Media**

1. Blogging by employees, whether using PrimeGov's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of PrimeGov's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate PrimeGov's policy, is not detrimental to PrimeGov's best interests, and does not interfere with an employee's regular work duties. Blogging from PrimeGov's systems is also subject to monitoring.
2. Employees are prohibited from revealing any PrimeGov confidential or proprietary information, trade secrets or any other material when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of PrimeGov and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or engaging on social media platforms.
4. Employees may also not attribute personal statements, opinions or beliefs to PrimeGov when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of PrimeGov. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, PrimeGov's trademarks, logos and any other PrimeGov intellectual property may also not be used in connection with any blogging activity.

**Policy Compliance****Compliance Measurement**

The policy owner will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

**Exceptions**

Any exception to the policy must be approved by the policy owner team in advance.

**Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**Related Standards, Policies and Processes**

*Password Protection Policy*

**Definitions and Terms**

The following definition and terms can be found in the SANS Glossary located at: <https://www.sans.org/security-resources/glossary-of-terms/>

- Honeypot
- Honeynet
- Proprietary Information
- Spam

# Password Protection Policy

## Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of PrimeGov's resources. All users, including contractors and vendors, with access to PrimeGov systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

## Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

## Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any PrimeGov facility, has access to the PrimeGov network, or stores any non-public PrimeGov information.

## Policy

### Password Creation

1. All user-level and system-level passwords must conform to the ***Error! Reference source not found.***
2. Users must not use the same password for PrimeGov accounts as for other non-PrimeGov access (for example, personal ISP account, option trading, benefits, and so on).
3. Where possible, users must not use the same password for various PrimeGov access needs.
4. User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user to access system-level privileges.
5. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet *Password Construction Guidelines*.

### Password Change

1. All system-level passwords (for example, root, enable, admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
2. All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.
3. Password cracking or guessing may be performed on a periodic or random basis by the policy owner or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with *Password Construction Guidelines*.

### Password Protection

1. Passwords must not be shared with anyone unless an exception is approved by the policy owner. All passwords are to be treated as sensitive, confidential PrimeGov information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
2. Passwords must not be inserted into email messages, support tickets or other forms of electronic communication.
3. Passwords must not be revealed over the phone to anyone, unless an exception is granted by the policy owner.
4. Do not reveal a password on questionnaires or security forms.
5. Do not hint at the format of a password (for example, "my family name").
6. Do not share PrimeGov passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
7. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
8. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.



## **Password Sharing**

In cases of unforeseeable circumstances (major issues, server down, etc.), the policy owner can grant an exception to share a password. On those scenarios:

1. Communicate passwords verbally, either in person or over the phone.
2. Communicate passwords through encrypted emails.
3. If none of the above are possible, communicate password through email, always separately from the username.

## **Application Development**

Application developers must ensure that their programs contain the following security precautions:

1. Applications must support authentication of individual users, not groups.
2. Applications must not store passwords in clear text.
3. Applications must not transmit passwords in clear text over the network.
4. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

## **Use of Passwords and Passphrases**

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The\*?#>\*@TrafficOnThe101WasT3rr1b!3ThisMorning"

All the rules above that apply to passwords apply to passphrases.

## **Policy Compliance**

### **Compliance Measurement**

The policy owner will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

### **Exceptions**

Any exception to the policy must be approved by the policy owner in advance.

### **Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## **Related Standards, Policies and Processes**

*Password Construction Guidelines*

## **Definition and Terms**

The following definition and terms can be found in the SANS Glossary located at <https://www.sans.org/security-resources/glossary-of-terms/>

- Simple Network Management Protocol (SNMP)

# Password Construction Guidelines

## Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network. This guideline provides best practices for creating secure passwords.

## Purpose

The purpose of this guidelines is to provide best practices for the creation of strong passwords.

## Scope

This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

## Policy

### Statement of Guidelines

Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include "It's time for vacation" or "block-curious-sunny-leaves". Passphrases are both easy to remember and type, yet meet the strength requirements.

Poor, or weak, passwords have the following characteristics:

- Contain eight characters or less.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Are some version of "Welcome123" "Password123" "Changeme123"

In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of 'password manager' software that is authorized and provided by the organization. Whenever possible, also enable the use of multifactor authentication.

## Policy Compliance

### Compliance Measurement

The policy owner will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

### Exceptions

Any exception to the policy must be approved by the policy owner in advance.

### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Related Standards, Policies and Processes

*Password Protection Policy*

## Definitions and Terms

None

# Data Protection Policy

## Overview

This policy refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality. With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

## Purpose

The purpose of this policy is to establish the requirement for all business units to follow when dealing with data they have gathered in the course of their daily activities and tasks related to their function within the organization.

## Scope

This policy refers to all parties (employees, job candidates, customers, suppliers etc.) who provide any amount of information to us. Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

## Policy

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, etc.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up to date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically, we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

## Actions

To exercise data protection we're committed to:

- Restrict and monitor access to sensitive data
- County of Orange - OCIT  
Prime Government Solutions LLC.

- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

## **Policy Compliance**

### **Compliance Measurement**

The policy owner will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

### **Exceptions**

Any exception to the policy must be approved by the policy owner in advance.

### **Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## **Related Standards, Policies and Processes**

None

## **Definition and Terms**

None

# Remote Access Policy

## Overview

Remote access to our corporate network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of PrimeGov policy, we must mitigate these external risks the best of our ability.

## Purpose

The purpose of this policy is to define rules and requirements for connecting to PrimeGov's network from any host. These rules and requirements are designed to minimize the potential exposure to PrimeGov from damages which may result from unauthorized use of PrimeGov resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical PrimeGov internal systems, and fines or other financial liabilities incurred as a result of those losses.

## Scope

This policy applies to all PrimeGov employees, contractors, vendors and agents with a PrimeGov-owned or personally owned computer or workstation used to connect to the PrimeGov network. This policy applies to remote access connections used to do work on behalf of PrimeGov, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to PrimeGov networks.

## Policy

It is the responsibility of PrimeGov employees, contractors, vendors and agents with remote access privileges to PrimeGov's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to PrimeGov.

General access to the Internet for recreational use through the PrimeGov network is strictly limited to PrimeGov employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the PrimeGov network from a personal computer, Authorized Users are responsible for preventing access to any PrimeGov computer resources or data by non-Authorized Users. Performance of illegal activities through the PrimeGov network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the Acceptable Use Policy.

Authorized Users will not use PrimeGov networks to access the Internet for outside business interests.

For additional information regarding PrimeGov's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., contact the department responsible.

## Requirements

1. Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong passphrases. For further information see the Password Protection Policy.
2. Authorized Users shall protect their login and password, even from family members.
3. All hosts that are connected to PrimeGov internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.
4. Personal equipment used to connect to PrimeGov's networks must meet the default requirements of PrimeGov-owned equipment for remote access.

## Policy Compliance

### Compliance Measurement

The policy owner will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and will provide feedback to the policy owner and appropriate business unit manager.

### Exceptions

Any exception to the policy must be approved by the policy owner in advance.

**Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**Related Standards, Policies and Processes**

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of PrimeGov's network:

- *Password Protection Policy*
- *Acceptable Use Policy*

**Definition and Terms**

None

# Server Security Policy

## Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

## Purpose

The purpose of this policy is to establish standards for the base configuration of internal or cloud server equipment that is owned and/or operated by PrimeGov. Effective implementation of this policy will minimize unauthorized access to PrimeGov proprietary information and technology.

## Scope

All employees, contractors, consultants, temporary and other workers at PrimeGov and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by PrimeGov or registered under a PrimeGov-owned internal network domain.

## Policy

### General Requirements

1. All internal servers deployed at PrimeGov or deployed in a cloud-based environment controlled by PrimeGov, must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides. The following items must be met:
  - Servers must be registered within the enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
  - Information in the corporate enterprise management system must be kept up to date.
  - Configuration changes for production servers must follow the appropriate change management procedures.
2. All servers deployed in a cloud-based environment controlled by PrimeGov should follow all the security recommendations and default security policies enabled by that cloud provider.
  - As of January 2020, we use Microsoft Azure and we're following all the system policies and recommendations.
3. For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic.

### Configuration Requirements

1. Operating System configuration should be in accordance with operating system vendor best practices.
2. Services and applications that will not be used must be disabled where practical.
3. Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
4. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
5. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
6. Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.
7. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
8. Servers should be physically located in an access-controlled environment.

9. Servers are specifically prohibited from operating from uncontrolled cubicle areas.

### **Monitoring**

1. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - All security related logs will be kept online for a minimum of 1 week.
  - Daily incremental tape backups will be retained for at least 1 month.

### **Policy Compliance**

#### **Compliance Measurement**

The policy owner will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

#### **Exceptions**

Any exception to the policy must be approved by the policy owner in advance.

#### **Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

### **Related Standards, Policies and Processes**

None

### **Definition and Terms**

None



# Security Response Plan Policy

## Overview

A Security Response Plan (SRP) provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, an SRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines. By requiring business units to incorporate an SRP as part of their business continuity operations and as new products or services are developed and prepared for release to consumers, ensures that when an incident occurs, swift mitigation and remediation ensues.

## Purpose

The purpose of this policy is to establish the requirement that the company develop and maintain a security response plan and all business units adhere to it unless it is determined that a different plan is needed for any of them. This ensures that security incident management team has all the necessary information to formulate a successful response should a specific security incident occur.

## Scope

This policy applies any established and defined business unity or entity within PrimeGov.

## Policy

The development, implementation, and execution of a Security Response Plan (SRP) are the primary responsibility of the Security Team in the case of the primary company SRP, and of the Head of the specific business unit for whom the SRP is being developed, in case of required deviations. Business units are expected to properly facilitate the SRP for applicable to the service or products they are held accountable. The business unit security coordinator or champion is further expected to work with the security team in the development and maintenance of a Security Response Plan.

## Service Product Description

The product description in an SRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams, architecture considered highly useful.

## Contact Information

The SRP must include contact information for dedicated team members to be available during non-business hours should an incident occur, and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact to customer. The SRP document must include all phone numbers and email addresses for the dedicated team member(s).

## Triage

The SRP must define triage steps to be coordinated with the security incident management team in a cooperative manner with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

## Identified Mitigations and Testing

The SRP must include a defined process for identifying and testing mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

## Mitigation and Remediation Timelines

The SRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company. These response guidelines should be carefully mapped to level of severity determined for the reported vulnerability.

## Policy Compliance

### Compliance Measurement

Each business unit must be able to demonstrate they have a written SRP in place, and that it is under version control and is available via the web. The policy should be reviewed annually.

**Exceptions**

Any exception to the policy must be approved by the policy owner in advance and have a written record.

**Non-Compliance**

Any business unit found to have violated (no SRP developed prior to service or product deployment) this policy may be subject to delays in service or product release until such a time as the SRP is developed and approved. Responsible parties may be subject to disciplinary action, up to and including termination of employment, should a security incident occur in the absence of an SRP.

**Related Standards, Policies and Processes**

None

**Definition and Terms**

None

## Appendix 2 – Agenda Database Structure for Data Migration Requirements

### AgendaWorks Search and Retrieval Database

**Total Number of Tables in the AgendaWorks Database: 15 tables**

Data dictionary (table names, field names, database relationship)

Data structure (including Entity Relationship diagrams, table names)

#### List of Tables to Migrate

Number	Table	Number of Records
1	Acting	
2	Agenda	
3	AgendaItems	
4	Agreement	
5	Dept	
6	Dictionary	
7	ImgFile	
8	Indexes	
9	ItemKeywords	
10	Minute	
11	Ordinance	
12	Resolution	
13	Status	
14	Type	
15	Vote	

### AgendaWorks Data Dictionary

Table	Column	Datatype	Size	Nullable	InPrimaryKey	IsForeignKey	Description
Acting	ActingId	Int	4	N	Y	N	
Acting	Seq	Numeric	5	N	N	N	
Acting	Name	VarChar (80)	80	N	N	N	
Agenda	Id	Int	4	N	Y	N	
Agenda	MeetDate	DateTime	8	N	N	N	
Agenda	TypeId	Int	4	N	N	N	
AgendaItems	Id	Int	4	N	Y	N	
AgendaItems	AgendaId	Int	4	N	N	Y	
AgendaItems	AgendaItemId	Int	4	N	N	N	
AgendaItems	ItemNo	Numeric	5	N	N	N	
AgendaItems	SItemNo	Char (10)	10	N	N	N	
AgendaItems	Subject	VarChar (80)	80	N	N	N	
AgendaItems	IndexId	Int	4	N	N	Y	
AgendaItems	TypeId	Int	4	N	N	Y	
AgendaItems	DeptId	Int	4	N	N	Y	
AgendaItems	ActingId	Int	4	N	N	Y	
AgendaItems	StatusId	Int	4	N	N	Y	
AgendaItems	Text	Text	16	N	N	N	
AgendaItems	AsrControlNo	Char (10)	10	N	N	N	
AgendaItems	RecommText	Text	16	N	N	N	
AgendaItems	deleted	Bit	1	N	N	N	

Agreement	Id	Int	4	N	Y	N
Agreement	ItemId	Int	4	N	N	Y
Agreement	AgreementNo	VarChar (50)	50	N	N	N
Dept	DeptId	Int	4	N	Y	N
Dept	Seq	Numeric	5	N	N	N
Dept	Name	VarChar (80)	80	N	N	N
Dictionary	Id	Int	4	N	Y	N
Dictionary	Keyword	VarChar (50)	50	N	N	N
ImgFile	Id	Int	4	N	Y	N
ImgFile	ItemId	Int	4	N	N	Y
ImgFile	ImgType	VarChar (50)	50	N	N	N
ImgFile	ImgPath	VarChar (150)	150	N	N	N
ImgFile	ImgName	VarChar (100)	100	N	N	N
ImgFile	ImgNoPages	Int	4	N	N	N
ImgFile	DocName	VarChar (50)	50	N	N	N
Indexes	IndexId	Int	4	N	Y	N
Indexes	Seq	Numeric	5	N	N	N
Indexes	Name	VarChar (80)	80	N	N	N
Indexes	NonItem	Bit	1	N	N	N
Indexes	AgendaTypeId	Int	4	N	N	N
ItemKeywords	Id	Int	4	N	Y	N
ItemKeywords	KeywordId	Int	4	N	N	Y
ItemKeywords	ItemId	Int	4	N	N	Y
ItemKeywords	SeqNo	Int	4	N	N	N
ItemKeywords	KeywordNo	Int	4	N	N	N
Minute	Id	Int	4	N	Y	N
Minute	ItemId	Int	4	N	N	Y
Minute	Disposition	Text	16	N	N	N
Minute	ApprAsRecomend	Bit	1	N	N	N
Minute	Other	Bit	1	N	N	N
Minute	Unanimous	Bit	1	N	N	N
Minute	MinuteOrder	Bit	1	N	N	N
Minute	BoardOrder	Bit	1	N	N	N
Minute	ConsentCal	Bit	1	N	N	N
Ordinance	Id	Int	4	N	Y	N
Ordinance	ItemId	Int	4	N	N	Y
Ordinance	Ordinance	VarChar (10)	10	N	N	N
Resolution	Id	Int	4	N	Y	N
Resolution	ItemId	Int	4	N	N	Y
Resolution	Resolution	VarChar (10)	10	N	N	N
Status	StatusId	Int	4	N	Y	N
Status	Seq	Numeric	5	N	N	N
Status	Name	VarChar (20)	20	N	N	N
Type	TypeId	Int	4	N	Y	N
Type	Seq	Numeric	5	N	N	N
Type	Name	VarChar (80)	80	N	N	N
Type	AgendaTypeId	Int	4	N	N	N
Vote	Id	Int	4	N	Y	N
Vote	MinuteId	Int	4	N	N	Y
Vote	DistrictNo	Int	4	N	N	N
Vote	Name	VarChar (50)	50	N	N	N
Vote	ActionId	Int	4	N	N	N



Appendix 2 - eAgenda Sample Feed to Creston

REGULAR MEETING OF THE BOARD OF SUPERVISORS

ORANGE COUNTY, CALIFORNIA

Tuesday, June 19, 2007

BOARD HEARING ROOM, FIRST FLOOR

333 W. Santa Ana Blvd., 10 Civic Center Plaza

Santa Ana, California

CHRIS NORBY  
CHAIRMAN  
Fourth District

JOHN M. W. MOORLACH  
VICE CHAIRMAN  
Second District  
JANET NGUYEN  
SUPERVISOR  
First District

BILL CAMPBELL  
SUPERVISOR  
Third District  
PATRICIA BATES  
SUPERVISOR  
Fifth District

COUNTY EXECUTIVE  
OFFICER  
COUNTY COUNSEL  
CLERK OF THE BOARD  
Thomas G. Mauk  
Benjamin P. de Mayo  
Darlene J. Bloom

The Orange County Board of Supervisors welcomes you to this meeting. This agenda contains a brief general description of each item to be considered. The Board of Supervisors encourages your participation. If you wish to speak on an item contained in the agenda, please complete a Speaker Form identifying the item(s) and deposit it in the Speaker Form Return box located on the side of the podium. If you wish to speak on a matter which does not appear on the agenda, you may do

so during the Public Comment period at the close of the meeting. Except as otherwise provided by law, no action shall be

taken on any item not appearing in the agenda. When addressing the Board, please state your name for the record. Please address the Board as a whole through the Chair. Comments to individual Supervisors or staff are not permitted. Speakers will be limited to three (3) minutes.

**\*\*In compliance with the Americans with Disabilities Act, those requiring accommodation for this meeting should notify the Clerk of the Board's Office 72 hours prior to the meeting at (714) 834-2206\*\***

All supporting documentation is available for public review in the office of the Clerk of the Board of Supervisors located in the Hall of Administration Building, 333 W. Santa Ana Blvd., 10 Civic Center Plaza, Room 465, Santa Ana, 92701 during regular business hours, 8:00 a.m. - 5:00 p.m., Monday through Friday. Agenda Items are also available online at <http://www.ocgov.com/supervisors/agenda/supervisorsagenda.asp>

9:30 A.M.

INVOCATION: Supervisor Nguyen, First District

PLEDGE OF ALLEGIANCE: Supervisor Campbell, Third District

**I N D E X**

I. PRESENTATIONS/INTRODUCTIONS	(None Scheduled)	Page #
II. CONSENT CALENDAR	(Items 1-65)	Page #
III. DISCUSSION ITEMS	(Items 66-103)	Page #
IV. PUBLIC HEARINGS	(Item 104)	Page #
V. CLOSED SESSION	(Items CS-1-CS-2)	Page #
VI. PUBLIC, CEO, BOARD & EMAIL COMMENTS & ADJOURNMENT		Page #

I. PRESENTATIONS/INTRODUCTIONS (None Scheduled)

II. CONSENT CALENDAR (Items 1-65)

All matters are approved by one motion unless pulled by a Board Member for discussion or separate action. At this time, any member of the public may ask the Board to be heard on any item on the Consent Calendar.

**BOARD APPOINTMENTS**

1.  
Supervisor Bates - Community Action Partnership of Orange County - Appoint Rhonda B. Reardon, Mission Viejo, for term ending 12/31/07

Supervisor Nguyen:

2.  
Development Processing Review Board - Reappoint Michael Recupero, San Juan Capistrano, for term concurrent with 1st District Supervisor's term of office

3.  
Orange County Human Relations Commission - Appoint Jim McQueen, Irvine,

4. Orange County Public Facilities Corporation - Appoint Art Pedroza, Santa Ana, for term concurrent with 1st District Supervisor's term of office

#### COMMENDATIONS/PROCLAMATIONS/REPORTS

5. Supervisor Bates - Adopt resolution proclaiming June 29 - July 5, 2007 as National Clean Beaches Week
6. Supervisor Nguyen - Adopt resolution acknowledging Pacifica High Drumline on Winning the World Championship title

#### ELECTED DEPARTMENT HEADS

7. Auditor-Controller - Acting as the Board of Supervisors and Orange County Flood Control District - Adopt resolutions establishing appropriations limits, cost of living and population factors, FY 2007-08 for County and Flood Control District funds - All Districts

#### Sheriff-Coroner:

8. Approve agreement with DMJM H&N, Inc. for design of James A. Musick Facility east kitchen rehabilitation project (\$174,818) - District 3 (Continued from 5/15/07, Item 3)
9. Approve standard agreement 70112111 with State of California for Commission on Peace Officer Standards and Training (P.O.S.T.) Basic Narcotics Investigation course, 7/1/07 - 6/30/08 and accept reimbursement for training costs (\$67,500); and authorize Director or designee to execute agreement and Form CCC-307, contractor certification clauses - All Districts
10. Approve agreement with DMJM H&N for design services for Theo Lacy Consolidated Maintenance project (\$98,875) - District 3
11. Authorize use of County vehicles and staff for transportation of Explorers to attend Channel Islands Explorer Challenge Competition, Oxnard, California 6/28/07 - 7/1/07; and the Colorado Western Regional Law Enforcement Explorer Conference, Denver, Colorado, 7/13/07 - 7/20/07; and make appropriate findings - All Districts
12. Receive bids and award contract to Delta Floors for replacement of carpeting, Brad Gates Forensics Building (\$174,194) - District 1

- 13.



Approve price agreement N1000008936 with Computer Concepts, Inc. for automated food services system software, 6/19/07 - 6/18/08 (\$264,010); renewable for four additional years per Board policy (\$52,258 second year, \$52,953 third year, \$53,660 fourth year, and \$54,406 fifth year) - All Districts

#### HEALTH CARE AGENCY

14.  
Approve agreement 06-00168 with State Department of Alcohol and Drug Programs for Substance Abuse Prevention & Treatment Federal Block Grant funds, FY 2007-08 (\$60,000) - All Districts

15.  
Approve price agreement N1000008738 with Atlas Development Corporation for web-based Confidential Morbidity Reporting software system, maintenance and support services per Board policy, 6/20/07 - 6/19/08 (\$186,457) - All Districts

16.  
Approve amended price agreement N1000007713 with California State University Long Beach Foundation for Tobacco Use Prevention program evaluation services, 7/1/07 - 8/31/08 (\$113,472) - All Districts

17.  
Approve agreement with Regents of the University of California for medi-Cal mental health managed care psychiatric inpatient hospital services, 7/1/07 - 6/30/08 (\$54,068) - All Districts

#### HOUSING AND COMMUNITY SERVICES DEPARTMENT

18.  
Approve amended Workforce Investment Act Cost Reimbursement agreement with Orange County Business Council to conduct labor market research projects, 7/1/07 - 12/31/07 (\$75,000); and authorize Director or designee to modify policies and procedures under certain conditions - All Districts

#### INTEGRATED WASTE MANAGEMENT DEPARTMENT

19.  
Adopt resolution certifying proposed Final SEIR 597, making findings set forth in "Statement of Findings and Fact in Support of Findings" and adopting Mitigation Monitoring and Reporting Program and Overriding Considerations with regards to amendment 2 to the 2001 Prima Deschcha Landfill General Development Plan; and make other California Environmental Quality Act findings - District 5

#### ORANGE COUNTY PUBLIC LIBRARY

20.  
Approve amended price agreement N1000008252 with Action 1st Loss Prevention for locksmith services, 12/1/06 - 11/30/07 (\$15,500; new total \$30,000); renewable for four additional one year terms per Board policy - All Districts

21.  
Direct Auditor-Controller to delete Hurricane Katrina Library Fund 2AK; and direct Treasurer-Tax Collector to pay residual balances and interest earnings to

RESOURCES AND DEVELOPMENT MANAGEMENT DEPARTMENT

22.  
Approve easement deed to Cox Communications for utility purposes, Laguna Coast Wilderness Park; and make California Environmental Quality Act findings - District 5
23.  
Receive bids and award contract to Best Contracting Services, Inc. for roof rehabilitation, Lamoreaux Justice Center (\$317,000) - District 3
24.  
Receive bids and award contract to Herk Edwards, Inc. for removal and replacement of fixed audience seating, Hall of Administration, and Central and Harbor Justice Centers (\$306,443) - Districts 1 & 2
25.  
Approve plans and specifications and set bid opening for 7/25/07, 2:00 p.m., for construction of multi-use trail, Laguna Coast Wilderness Park; and find that EIR 556 and Addendums IP 00-143, IP 01-031 and IP 02-170 and Final Mitigated Negative Declaration No. IP 05-05-036 are adequate to satisfy requirements of California Environmental Quality Act findings - District 5
26.  
Approve assignment of agreement from Klassic Engineering to H. L. Miller for construction of custody boxes and separation areas, Superior Court Harbor Justice Center (\$121,391); and authorize Auditor-Controller to make related payments - District 2
27.  
Approve agreement with KPFF Consulting Engineers for replacement of pedestrian bridge, Arden/Modjeska Historic House and Garden (\$93,093); and make California Environmental Quality Act findings - District 3
28.  
Approve plans and specifications and set bid opening for 7/25/07, 2:00 p.m., for widening of Irvine Avenue from Mesa Drive to Bristol Street; and make California Environmental Quality Act findings - District 2
29.  
Approve amendment 3 to agreement D98-072 with Orange County Transportation Authority for partial funding of Laguna Canyon Road project, extending term to 6/30/09 - District 5
30.  
Approve agreement D07-034 with Huitt-Zollars, Inc. for on-call professional engineering services for Harbors, Beaches and Parks restoration and capital projects, three-year term (200,000); and make California Environmental Quality Act findings - All District
31.  
Receive bids and award contract to GCI Construction, Inc. for Brenan Way

drainage improvements and pavement overlay, North Foothill area (\$468,978) -  
Attachment Contract MA-072001143 -  
District 3

32.  
Receive bids and award contract to J. Kim Electric, Inc. for replacement of master controlled lighting system with individual lighting controls, Probation Headquarters (\$121,500) - District 1

33.  
Receive bids and award contract to Leo's A-C, Inc. for painting of restrooms and common areas, various Civic Center buildings (\$41,000) - District 1

34.  
Declare bid of Generator Services Company to be non-responsive; receive bids and award contract to Allied Industrial Systems, Inc. for rehabilitation of six generators at various locations (\$189,000) - Districts 1 & 3

35.  
Adopt resolution accepting Cove Road, Dana Drive, Island Way and a portion of Dana Point Harbor Drive into the Orange County Road System; and make California Environmental Quality Act findings - District 5

36.  
Declare bid of Generator Services Company to be non-responsive; receive bids and award contract to Allied Industrial Systems, Inc. for Data Center generator rehabilitation (\$198,000) - District 1

37.  
Receive bids and award contract to KDC, Inc. dba Dynalectric for replacement of electrical equipment, Irvine Regional Park (\$145,830) - District 3

38.  
Select Norris-Repke as firm for building plan check services; and authorize negotiation of agreement for Board approval - All Districts

39.  
Receive bids and award contract to S&S Power Engineering, Inc. for replacement of uninterruptible power supply, Building 12 (\$153,109) - District 1

40.  
Receive bids and award contract to H.L. Miller, Inc. for construction of restrooms, Joplin Youth Center (\$115,000) - District 3

41.  
Approve Parcel Map 2004-274, James and Linda Hill, East Orange area; accept dedication of street purposes; and accept vehicular access rights to Crawford Canyon Road - District 3

42.  
Approve amended license agreement with Orange County Transportation Authority for Poche Beach Ultraviolet Bacteria Disinfection System project - District 5

43.  
Approve Tract 17034, Signal Landmark, a California Corporation, Huntington

Beach area; accept easements for pedestrian, bicycle, and vehicle ingress and egress sewer and water, and fire access purposes; approve construction agreement S0307-0145 and accept bonds guaranteeing construction improvements - District 2

44.  
Approve lease with Jesus Baptist Los Angeles Church for use of additional rentable office space located at 1530-1540 E. First Street, Santa Ana; and make California Environmental Quality Act findings - District 1

45.  
Accept work of Exbon Development, Inc. for rehabilitation of shelter roofs, Laguna Niguel Regional Park, project completed 5/21/07 (\$156,949) - District 5

46.  
Receive bids and award contract to Christopher R. Morales, Inc. for installation of in-roadway flashing crosswalk light system for Hewes Avenue at Spaulding Avenue and Red Hill Avenue at Bullard Lane, North Tustin area (\$128,860) - District 3

47.  
Approve County 7-Year Transportation Capital Improvement Program for submittal to Orange County Transportation Authority for Measure M funds - All Districts

48.  
Acting as the Orange County Flood Control District - Approve agreement D07-027 with Steinberg & Associates for technical assistance and support matters relating to federal funding for flood control, water quality improvement and watershed protection in Orange County, three-year term (\$200,000); and make California Environmental Quality Act findings - All Districts

49.  
Acting as the Board of Supervisors and Orange County Development Agency - Acting as Board of Supervisors - receive bids and award contract to Hanan Construction Company, Inc. for remodeling of Anaheim Independencia Community Center (\$288,000); and Acting as the Board of Supervisors and the Orange County Development Agency - adopt resolutions pursuant to Health and Safety Code Section 33445 relating to Independencia Community Center Remodel Project - District 4

## SOCIAL SERVICES AGENCY

50.  
Approve amended price agreement N1000007460 with Alquest Technologies Inc. for Information Technology/Telephone Services communication network maintenance, 7/1/07 - 6/30/08 (\$240,000) - All Districts

51.  
Approve agreement MER0307 with Goodwill Industries of Orange County for sign language interpretation services, 7/1/07 - 6/30/08 (\$70,000); and authorize Director or designee to renew agreement for two additional one year terms per Board policy - All Districts

52.

Approve agreement WAA1107 with People For Irvine Community Health dba 2-1-1 Orange County to provide information and referral database services, 7/1/07 - 6/30/08 (\$121,400); and authorize Director or designee to extend terms and conditions twelve additional months without further Board action - All Districts

53.

Approve price agreement N1000008846 with International Business Machine dba IBM Corporation for weekly American Standard Code for Information Interchange downloads of Child Welfare Services/Case Management System data, 7/1/07 - 6/30/12 (\$250,000) - All Districts

54.

Approve Memorandum of Understanding MHT0207 with California Ventura Automated Collections System to continue participation in California Ventura Automated Collection System Association, 7/1/07 - 6/30/08 (\$11,542.92); and authorize Director or designee to renew agreement for two additional one year terms per Board policy - All Districts

55.

Approve agreement WMR0107 with California State Association of Counties for management of Welfare Client Data Systems, 7/1/07 - 6/30/08 (\$78,833); and authorize Director or designee to execute subsequent amendments under certain conditions - All Districts

## PUBLIC PROTECTION

### Probation:

56.

Approve agreement with Orange County Superintendent of Schools for provision of Deputy Juvenile Correctional Officer II and Supervising Probation Officer services for High-Risk Youth Education and Public Safety Program, 7/1/07 - 6/30/08 (\$326,511); and make California Environmental Quality Act findings - Districts 1 & 4

57.

Approve agreement with Orange County Superintendent of Schools for the provision of Supervising Probation Officer services under the Foster Youth Services Program, 7/1/07 - 6/30/08 (\$20,000); and make California Environmental Quality Act findings - All Districts

58.

Adopt resolution ratifying execution and submission of grant award agreement RT05060300 with State Office of Emergency Services for Residential Substance Abuse Treatment services, term ending 6/30/07 (\$180,000; new total \$282,180); make related budget adjustments; and make California Environmental Quality Act findings - All Districts (4/5 vote)

59.

Approve agreement with Costa Mesa for provision of gang prevention and suppression services, 7/1/07 - 6/30/08 (\$126,927); authorize Chief Probation Officer to execute agreement; and make California Environmental Quality Act findings - District 2

60. Approve Memorandum of Understanding with Orange County Bar Foundation for provision of community reintegration services under the Youth Transitional Intervention Program for voluntary participation by minors housed at Youth Guidance Center, 7/1/07 - 6/30/08; authorize Chief Probation Officer to renew MOU two individual consecutive one year terms under certain conditions; and make California Environmental Quality Act findings - All Districts

#### GENERAL ADMINISTRATION

County Executive Office:

61. Approve price agreement N1000008874 with Govplace, Inc. for Information Technology Portfolio Management Solution, 6/19/07 - 6/18/08 (\$393,389); renewable for two additional one-year periods (\$30,016 per year), per Board policy - All Districts

62. Adopt resolution superseding portions of Resolution 00-202 and revising Workers' Compensation Claims settlement procedures to authorize CEO/Risk Management to settle workers' compensation claims if settlement amount is less than \$100,000, excluding statutorily required payments pursuant to Labor Code - All Districts (Continued from 6/5/07, Item 44)

63. Approve price agreement N1000008932 with McAfee, Inc., for County-Wide Information Technology Security Audit, 6/19/07 - 3/31/08 (\$337,450) - All Districts

Supervisor Norby:

64. Approve waiver of permit and parking fees for Karnataka Cultural Association of Southern California, a non-profit organization for picnic event on 7/1/07 at Ralph E. Clark Regional Park, Buena Park

65. Approve waiver of permit and parking fees for Golden Hearts, a support group of St. Jude Memorial Foundation picnic event on 9/30/07 at Ralph E. Clark Regional Park, Buena Park  
END OF CONSENT CALENDAR

#### III. DISCUSSION ITEMS (Items 66-103)

At this time, members of the public may ask the Board to be heard on the following items as those items are called.

#### ELECTED DEPARTMENT HEADS

66. Treasurer-Tax Collector - Consider second reading and adoption of "An Ordinance of the County of Orange, California Amending Sections 8-1-17 and 8-1-18 of the Codified Ordinances of the County of Orange to Increase the Fees for

Seizure of Property and Execution on Accounts in Financial Institutions by the  
Treasurer-Tax Collector and Adding Section 8-1-21 to the Codified Ordinances of  
the County of Orange to Establish Fee for Processing by the Treasurer-Tax  
Collector of Requests to Pay Delinquent Taxes in Installments" - All Districts  
(Closed Public Hearing and continued from 6/5/07, Item 68)

## HEALTH CARE AGENCY

67.  
Approve amendment 6 to price agreement S4000000250 with Cerner Corporation  
for renewal of annual maintenance fees, 7/1/07 - 6/30/08 (\$1,350,265) - All  
Districts
68.  
Approve amended A1 agreements with State Department of Alcohol and Drug  
Programs for Comprehensive Drug Court Implementation Grant funds, 12/29/05 -  
6/30/07 (\$5,584; new total \$698,576) and Drug Court Partnership Grant funds,  
7/1/05 - 6/30/07 (\$26,164; new total \$451,339); and authorize Director or designee  
to execute agreements - All Districts
69.  
Approve agreements with AIDS Services Foundation Orange County (\$295,000),  
Special Service for Groups (\$51,000) and The Gay and Lesbian Community  
Services Center of Orange County (\$150,000) for HIV Prevention services, 7/1/07 -  
6/30/08 - All Districts
70.  
Approve amended price agreement N1000007803 with AT&T Datacomm, Inc., for  
network equipment maintenance and support services, 7/1/07 - 6/30/08 (\$217,566) -  
All Districts
71.  
Approve amended price agreement N2000006840 with United Maintenance  
Systems for janitorial services, 7/1/07 - 6/30/08 (\$189,000) per Board policy -  
District 1
72.  
Approve agreement with Orange County Asian and Pacific Islander Community  
Alliance for Full Service/Wraparound Program for Children and Transitional Age  
Youth, 7/1/07 - 6/30/09 (\$2,000,000) - All Districts
73.  
Approve agreements with Behavioral Health Services, Inc. (\$358,613), Social  
Model Recovery Systems, Inc. (\$1,018,038) and Southern California Alcohol and  
Drug Programs, Inc. (\$2,769,852) for alcohol and drug abuse services, 7/1/07 -  
6/30/09; and approve master agreements with various providers for post custody re-  
entry services for substance abusers, 7/1/07 - 6/30/09 (\$1,120,402) and alcohol and  
drug abuse drinking driver programs, 7/1/07 - 6/30/08; and authorize Director or  
designee to execute individual agreements - All Districts
74.  
Approve agreement with Community Service Programs, Inc., for alcohol, tobacco,  
and other drug prevention services, 7/1/07 - 6/30/09 (\$190,000); and approve  
agreements with Orange County Superintendent of Schools for alcohol, tobacco,

and other drug prevention poster contest services (\$200,000) and Friday Night Live Partnership, 7/1/07 - 6/30/09 (\$900,000)- All Districts

## HOUSING AND COMMUNITY SERVICES DEPARTMENT

75.

Adopt resolution adopting Workforce Investment Act subgrant agreement with State Employment Development Department for Workforce Investment Act services, FY 2006-07; and authorize Director or designee to execute subsequent amendments and related documents under certain conditions - All Districts

76.

Approve Workforce Investment Act Cost Reimbursement agreements with Coast Community College District to operate the Northern Region Business Service Center (\$425,000) and with Arbor E&T, LLC to operate the Southern Region Business Service Center (\$425,000), 7/1/07 - 6/30/08; and authorize Director or designee to modify policies and procedures under certain conditions - All Districts

77.

Approve agreements with Community Service Programs, Inc. (\$162,547), Council of Orange County, Society of St. Vincent de Paul (\$174,314), Fair Housing Council of Orange County (\$119,000) and Orange County Human Relations Council (\$167,139) for dispute resolution program services, 7/1/07 - 6/30/08; and authorize Director or designee to modify scope of services - All Districts

78.

Approve Workforce Investment Act Cost Reimbursement agreements with various providers for In-School Youth program (\$748,611) and Out-of-School Youth program (\$1,122,917), 7/1/07 - 6/30/08; and authorize Director or designee to modify policies and procedures and agreement without Board action under certain conditions - All Districts

79.

Approve Workforce Investment Act Cost Reimbursement agreements with Coast Community College District to operate Northern and Southern Regions Orange County One-Stop Centers (\$2,815,132 for northern and \$2,064,336 for southern); and authorize Director or designee to modify Workforce Investment Act policies and procedures - All Districts

80.

Approve agreements with various providers for domestic violence shelter-based services, 7/1/07 - 6/30/08 (\$967,000); and authorize Director or designee to amend scope of agreements under certain conditions - All Districts

81.

Approve use of funds from State of California Mental Health Service Act for Diamond Aisle Apartments, Anaheim (\$1,029,600); authorize Director to prepare and execute loan documents, restrictive covenants, subordination agreements and related documents - District 4

82.

Approve standard agreements AP-0708-22, HI-0708-22 and TV-0708-22 with State Department of Aging, amendment 4 to agreements with Orange County Transportation Authority and St. Jude Hospital/Orange Caregiver Resource Center,



amendment 3 to agreement with Barbara J. Woodruff and agreements with various providers for senior services, FY 2007-08; and authorize Director or designee to execute agreements and subsequent amendments under certain conditions - All Districts

83.

Approve fourth and fifth amendments to agreements with St. Anselm's Cross-Cultural Community Center, Inc., St. Jude Hospital, Inc. and South County Senior Services, Inc. for Senior Non-Emergency Medical Transportation services, 7/1/07 - 12/31/07; authorize Housing and Community Services Department and Health Care Agency to develop plan to address funding limitations and return to Board with recommendations; and authorize Director or designee to execute agreements and subsequent amendments under certain conditions - All Districts

#### INTEGRATED WASTE MANAGEMENT DEPARTMENT

84.

Approve agreement with Bryan A. Stirrat & Associates to provide construction management, quality assurance/quality control and archaeological/paleontological services, South Region Landfills, three year term (\$2,400,000) - District 5

#### JOHN WAYNE AIRPORT

85.

Select Walker Parking Consultants as primary and Watry Design, Inc. as alternate firms to perform design and construction administration services for B1 Parking Structure project; authorize negotiation of agreement for Board approval; and find Final EIR 582 and addendum 582-1 are adequate to satisfy requirements of California Environmental Quality Act - District 2

86.

Approve agreement with Gensler for design and construction administration services for new Terminal C and renovation of Terminals A and B (\$26,395,503); and find Final EIR 582 and addendum 582-1 are adequate to satisfy requirements of California Environmental Quality Act findings - District 2

#### ORANGE COUNTY PUBLIC LIBRARY

87.

Approve amended price agreement N2000006726 with Online Computer Library Center for on-line cataloging, interlibrary loan and related services, 7/1/07 - 6/30/08 (\$130,000) - All Districts

#### RESOURCES AND DEVELOPMENT MANAGEMENT DEPARTMENT

88.

Acting as the Orange County Flood Control District - Approve acquisition contract and accept grant deed from Pearl Ann Neiderhiser for purchase of real property in the Prado Dam Basin area (\$480,000); authorize Director or designee to execute related documents; authorize Auditor-Controller to make related payments; and make California Environmental Quality Act findings - All Districts

#### SOCIAL SERVICES AGENCY

89.

Approve agreement MAA0107 with Public Health Foundation Enterprises, Inc., dba PHFE Management Solutions for Children's Outreach, Enrollment, Retention, and Utilization services for Medi-Cal and Healthy Families Programs, 7/107 - 6/30/08 (\$2,004,663); and authorize Director or designee to extend term for twelve additional months without Board action under certain conditions - All Districts

90.

Approve agreements CHT2007 with National Pediatric Support Services (\$60,000) for Team Decision Making Child Care services, CHT2107 with Orange County Child Abuse Prevention Center for Volunteer Advocacy services (\$80,000), CLC2407 with Holy Family Services for In-Home Adoption services and CLC2307 with Kinship Center for In-Office Adoption Counseling (\$150,000), 7/1/07 - 6/30/08; and authorize Director or designee to extend terms for twelve additional months under certain conditions without further Board action - All Districts

91.

Approve agreements with various providers for child abuse prevention and intervention, emancipation and independent living program, and other supportive services, 7/1/07 - 6/30/08 (\$8,722,444); and authorize Director or designee to extend terms for twelve additional months under certain conditions without further Board action; approve funding allocation for private sector counseling services, FY 2007-08 (\$934,702); and receive and file The Raise Foundation Annual Report - All Districts

92.

Approve standard agreement MS-0708-18 with State Department of Aging (\$1,542,600) and agreements AER0107 with Rosemary Rodriguez dba Catalina Health Care and AER0207 with Long Beach Oxford Services, Inc. dba Oxford Services (\$100,000) for Multipurpose Senior Services Program services, 7/1/07 - 6/30/08; and authorize Director or designee to execute related documents - All Districts

93.

Acting as the Board of Supervisors and OC In-Home Supportive Services Public Authority - Approve interagency agreement AEH0307 with Orange County In-Home Supportive Services Public Authority for In-Home Support services, 7/1/07 - 6/30/08; and authorize Director to execute Memorandum of Agreement AEH0407 to continue appointment of Robert D. Miller as Executive Director of Orange County In-Home Supportive Services Public Authority - All Districts

## PUBLIC PROTECTION

### Probation:

94.

Approve lease with Anaheim Business Campus, LLC for Probation Department's North O. C. Youth & Family Resource Center, 7/1/07 - 6/30/10; and make California Environmental Quality Act findings - District 4

95.

Authorize Chief Probation Officer, Director of Health Care Agency, District Attorney, Public Defender and Sheriff-Coroner to execute Joint Letter of Agreement with Superior Court of California to implement terms of State grant

for DUI offenders, 1/12/07 - 9/30/08 (\$926,750); and make California Environmental Quality Act findings - Districts 2, 3 & 4

## GENERAL ADMINISTRATION

96.  
County Counsel - Consider first reading of "An Ordinance Amending Section 1-2-1 of the Codified Ordinances of the County of Orange, Regarding the Time and Place of Regular Meetings"; and set second reading and adoption for 6/26/07, 9:30 a.m. - All Districts

County Executive Office:

97.  
Approve recommended positions on introduced or amended legislation and consider other legislative subject matters - All Districts

98.  
Approve proposed response to FY 2006-07 Grand Jury Report "Offices of the Public Defender" - All Districts

99.  
Approve Strategic Investment Solutions, Inc. as firm to review and report on the Orange County Employees Retirement System investment portfolio; and authorize negotiation of agreement for Board approval - All Districts

100.  
Adopt resolution amending and restating County of Orange Retiree Medical Plan; establishing County of Orange Retiree Medical Trust; adopting certain administrative, Internal Revenue Code, Section 401 (h) account and investment agreements with Orange County Employees Retirement System; and taking other actions and approving other related documents and matters as specified in resolution - All Districts

101.  
Adopt "Policy for Use of County Vehicles by Staff for Non-County Events or Transportation of Volunteers, Etc." - All Districts

102.  
Approve amendment 2 to Memorandum of agreement with Newport Beach for purchasing land for and constructing a fire station and recreation facility, Santa Ana Heights area - District 2

103.  
Human Resources Department - Select Blue Shield of California as primary and Blue Cross of California as alternate firms for County self-insured Preferred Provider Organization Health Plans and Management and Attorney Dental Plan; and authorize negotiation of agreement for Board approval - All Districts

## IV. PUBLIC HEARINGS (Item 104)

## GENERAL ADMINISTRATION

104.  
County Executive Office - Public Hearing to consider adopting resolution authorizing Southern California Home Financing Authority to issue single family mortgage revenue bonds to fund Home Financing Program; and make appropriate findings - All Districts

V. CLOSED SESSION (Items CS-1-CS-2)

The Board will break for lunch at approximately 12:00 PM and may consider closed session matters during that break. The Board will then resume to handle any remaining business if necessary.

GENERAL ADMINISTRATION

County Counsel:

CS-1.  
CONFERENCE WITH LEGAL COUNSEL - EXISTING LITIGATION -  
Pursuant to Government Code Section 54956.9(a):  
Name of Case: C.A. Rasmussen, Inc. v. Irvine Community Development Company, et al., Orange County Superior Court Case No. 01CC01143

CS-2.  
CONFERENCE WITH LEGAL COUNSEL - EXISTING LITIGATION -  
Pursuant to Government Code Section 54956.9(a):  
Name of Case: Tyson Lewis v. County of Orange, Orange County Superior Court Case No. 06CC11236

VI. PUBLIC, CEO, BOARD & EMAIL COMMENTS & ADJOURNMENT

PUBLIC COMMENTS:

At this time, members of the public may address the Board of Supervisors regarding any off-agenda items within the subject matter jurisdiction of the Board of Supervisors provided that NO action may be taken on off-agenda items unless authorized by law. Comments shall be limited to three minutes per person and twenty minutes for all comments, unless different time limits are set by the Chairman subject to the approval of the Board.

COUNTY EXECUTIVE OFFICER COMMENTS:

BOARD COMMENTS:

At this time, members of the Board of Supervisors may comment on agenda or non-agenda matters and ask questions of or give directions to staff; provided that NO action may be taken on off-agenda items unless authorized by law.

ADJOURNED:

NEXT MEETINGS:  
June 26, 2007 Regular Meeting  
July 3, 2007 Canceled Meeting



**PRIMEGOV SERVICE AGREEMENT ("Agreement")**

**THIS AGREEMENT** is made on the \_\_\_\_\_ day of \_\_\_\_\_ 20\_\_\_\_  
**BETWEEN**

- 1. **PRIME GOVERNMENT SOLUTIONS LLC**, a Utah Limited Liability Company having its principal office at 220 N. 1200 E. #201, Lehi, UT 84043 (the **"Supplier"**); and
- 2. \_\_\_\_\_, whose registered office is at \_\_\_\_\_ (the **"Customer"**)  
(and at times referred to in this Agreement as a "party" or "parties")

**BACKGROUND**

- A. The Supplier has developed and owns the Service (as defined in clause 1) and has granted to the Customer a non-exclusive license to use such Service solely for Customer's internal operations and in accordance with the terms and conditions of this Agreement. The terms of this Agreement shall also apply to any updates and upgrades subsequently provided by Supplier to Customer for the Service. Supplier may update the functionality of or make modifications to the Service and user interface of the Service from time to time in its sole discretion and shall not be liable to Customer or to any third party for any modification of the Service. Supplier will use commercially reasonable efforts to notify Customer of any material modifications.
- B. The Customer wishes the Supplier to provide certain support services in respect of the Service in accordance with the provisions set out in Schedule 1 of this Agreement ("Support Services").

**OPERATIVE PROVISIONS**

**1 DEFINITIONS**

In this Agreement the following expressions will have the following meanings unless inconsistent with the context:

- "Affiliate"** means any company or non-corporate entity that controls, is controlled by, or is under common control with a party. An entity shall be regarded as in control of another company or entity if it owns or directly or indirectly controls more than 50 per cent. of the voting rights of the other company or entity
- "Application Password"** means any encryption keys, certificates, passwords, access codes, user IDs or other login information provided to or used by Customer for the purpose of accessing and using the Service.
- "Business Day"** a day that is not a Saturday, Sunday, or public holiday.
- "Client Environment"** means the Customer hardware and software system containing the minimum specification, which the Customer, as advised by Supplier, is required to have to enable the Customer to connect with the Service.
- "Customer Data"** means data, information or material provided or submitted by Customer or any User to the Supplier in the course of utilizing the Service.
- "Effective Date"** means the date of this Agreement signed by the Supplier and the Customer.
- "Intellectual Property Rights"** means all intellectual and industrial property rights of any kind whatsoever, registered or unregistered, including patents, know-how, software, code, intellectual property specifications, design plans, prototypes, drawings, software, software documentation, material, documents, ideas, operations, processes, product information, know-how, and the like including mode and procedures of development of source code, registered trademarks, registered designs, utility models, applications for and rights to apply for any of the foregoing, unregistered design rights, unregistered trademarks, rights to prevent passing off for unfair competition and copyright, database rights, topography rights, and any other rights in any invention, discovery or process, in each case in all countries in the world and together with all renewals and extensions.
- "Pricing Schedule"** means Schedule 2 to this Agreement which sets out the prices and payment terms for the Service.
- "Professional Services"** means the general consulting, implementation and/or training services to be provided to Customer.
- "Purchase Order"** means a purchase order issued by the Customer to the Supplier for the Service.
- "Service"** means Supplier's online software applications purchased by Customer and maintained through Support Services by Supplier including associated offline components and ancillary online or offline services to which Customer is granted access under this Agreement.

<b>“Service Level Commitments”</b>	the service level commitments in respect of the Service to the Customer as more particularly set out in Schedule 1.
<b>“Term”</b>	means the term of this Agreement as specified in clause 3.
<b>“User”</b>	means one (or if more than one “Users”) of Customer’s employees, representatives, consultants, contractors or agents and other persons expressly permitted by Customer in connection with Customer’s business affairs who are authorized to use the Service and have been supplied User identifications and passwords by Customer.

## 2 INTERPRETATION

- 2.1 Person:** The expression “person” means any individual, firm, body corporate, unincorporated association, or partnership, government, state or agency of a state or joint venture.
- 2.2 Headings:** The index and headings to the clauses, the Appendices and Schedules of this Agreement are for convenience only and will not affect its construction or interpretation.
- 2.3 Statutes:** Any reference to a statute or statutory provision and all regulations and notices made pursuant to it (whether made before or after the date of this Agreement), includes a reference to the same as from time to time amended, modified, extended, re-enacted, consolidated, or replaced provided that amendments, consolidations, modifications, extensions, re-enactments or replacements made after the date of this Agreement will not have substantively changed any provision which is relevant to this Agreement.
- 2.4 Provisions of the Agreement**
- 2.4.1** Any reference in this Agreement to a clause, Schedule or Appendix is a reference to a clause, Schedule or Appendix of this Agreement and references in any Schedule or Appendix to paragraphs relate to the paragraphs in that Schedule or Appendix.
- 2.4.2** The Schedules and Appendices form part of this Agreement and will have the same force and effect as if expressly set out in the body of this Agreement and any reference to this Agreement will include the Schedules and Appendices.
- 2.5 Writing:** Any references to “writing” or “written” includes references to any communication effected by post, facsimile, email or any comparable means.

## 3 TERM

- 3.1** This Agreement shall unless terminated in accordance with clause 19, commence on the Effective Date and shall continue for an initial period of 3 years therefrom (the “**Initial Term**”).

## 4 CUSTOMER USE OF THE SERVICE

- 4.1** Supplier grants Customer a license to access and use the Service during the Term via the internet under and subject to the terms of this Agreement. Supplier reserves the right to make changes and updates to the functionality and/or documentation of the Service from time to time.

## 5 FEES AND PAYMENT

- 5.1** Customer agrees to pay fees as set forth in the Pricing Schedule. (“the Service Fees”).
- 5.2** The Service Fees shall be billable and payable annually in advance for a twelve (12) month period at a time (“a Service Year”) on the anniversary of the Effective Service Date (“the “Renewal Date”) for the first year and for each year thereafter the Service Fees shall be payable annually in advance on each subsequent anniversary of the Renewal Date. One month prior to the expiry of a Service Year (“Service Year Expiry Date”) the Service Fees for the Service Year will be invoiced by the Supplier to the Customer in respect of the Service to be provided in the following Service Year. The Customer shall pay the Service Fees on or before the relevant Service Year Expiry Date.
- 5.3** Where any additional Service(s) is acquired by the Customer during the period between one Renewal Date and the next Renewal Date (“the Installation Year”) the Service Fees payable shall be calculated pro-rata, from the date of the Purchase Order for the Service(s) in the Installation Year up to the next Renewal Date applicable to Customer’s other Licenses. For all subsequent years thereafter, the Service Fees shall be payable annually in advance on each anniversary of the Renewal Date in accordance with this Agreement.
- 5.4** Where the Supplier performs Professional Services under this Agreement (such as configuration of the Support Service if requested by Customer or migration of Customer Data to the Service), such services shall be invoiced by the Supplier on a time and material basis in accordance with the Supplier’s rates in effect at the time of provision of such services (“Professional Services Fees”) unless otherwise agreed in writing between the Parties and will be payable without withholding, deduction or off set of any amounts for any purpose.
- 5.5** The Service Fees and Professional Service Fees do not include local or foreign taxes, duties, fees and levies imposed from time to time by any government or other authority (“Taxes”) and such Taxes, where applicable, will be payable by the Customer on the Service Fees and Professional Services Fees, at the rate applicable at the time of supply of the Service and/or Professional Services.
- 5.6** Customer agrees to provide Supplier billing and contact information as Supplier may reasonably require. Customer agrees to update this information promptly by means of email to the Supplier and in any case within 15 days, if there is any change.

## 6 NON-PAYMENT

- 6.1** Customer’s account will be considered delinquent (in arrears) if the Supplier has not received payment in full within 30 days after the due date, and without prejudice to any other rights and remedies of the Supplier;

### 6.1.1

- 6.1.2** Subject to clause 6.4 below, the Supplier may, upon giving ten (10) days written notice but without liability to the Customer, disable/suspend the Customer’s password, account and access to all or part of the Service and the Supplier shall be under no obligation to provide any or all of the Service while the invoice(s) or any part thereof, remains unpaid;

- 6.2 Supplier may in its discretion, decide not to exercise its rights under clause 6.1.1 (interest) and 6.1.2 (suspension), if Customer is disputing the applicable Service Fees and/or Professional Services Fees reasonably and in good faith and is cooperating diligently to resolve the dispute.
- 6.3 Supplier reserves the right to impose a reconnection fee if the Service is suspended (as a result of Customer's breach) but subsequently reinstated.
- 6.4 Without recourse to clause 6.1.2, Supplier reserves the right to terminate this Agreement if Customer's account falls into arrears 30 days after the due date.

## 7 RESTRICTIONS ON USE OF THE SERVICE

- 7.1 The Customer may not: -
  - 7.1.1 make the Service or use the Service for the benefit of anyone else other than the Customer and the Customer's Users. Customer shall access and use the Service only to the extent of authorizations acquired by the Customer in accordance with this Agreement (for example the quantity specified in the relevant Purchase Order) and Customer agrees that the Customer is solely responsible for use of the Service by any Users who access and/or use the Service. Customer agrees to immediately notify the Supplier if Customer becomes aware of any loss or theft or unauthorized use of Customer's account credentials.
  - 7.1.2 sublicense, resell or supply the Service for use in or for the benefit of any other organization, entity, business, or enterprise without Supplier's prior written consent.
  - 7.1.3 submit to the Service any material that is illegal, defamatory, threatening, infringing of any third-party proprietary rights, invasive of personal privacy, (collectively "Objectionable Matter").
  - 7.1.4 interfere with or disrupt the integrity or attempt to gain unauthorized access to the Service or the Supplier's intellectual property therein;
  - 7.1.5 copy the Service or any part, feature, function or user interface thereof;
  - 7.1.6 frame or mirror any part of any Service on any other server or wireless or internet-based device outside of the agreed usage in this contract;
  - 7.1.7 access any part of the Service in order to build a competitive product or service or to build a product using similar ideas, features, functions or graphics of the Service;
- 7.2 Supplier reserves the right to disable, suspend or terminate this Agreement for cause in case the Customer breaches the provisions of this clause 7.

## 8 CUSTOMER DATA

- 8.1 The Customer shall own all rights, title and interest in and to all of the Customer Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the Customer Data.
- 8.2 Supplier will use best efforts to provide protection using current technological standards to protect Customer Data against unauthorized disclosure or use.
- 8.3 In the event of any loss or damage to Customer Data, the Customer's sole and exclusive remedy shall be for the Supplier to use reasonable commercial endeavors to restore the lost or damaged Customer Data from the latest back-up of such Customer Data maintained by the Supplier. The Supplier shall not be responsible for any loss, destruction, alteration or disclosure of Customer Data caused by any third party (except those third parties sub-contracted by the Supplier to perform services related to Customer Data maintenance and back-up).
- 8.4 Subject to the terms and conditions of this Agreement, Customer grants to Supplier a non-exclusive license to use, copy, store, transmit and display Customer Data to the extent reasonably necessary to provide and maintain the Service.

## 9 CUSTOMER'S OBLIGATIONS

- 9.1 The Customer shall:
  - 9.1.1 provide the Supplier with:
    - (i) all necessary co-operation in relation to this Agreement; and
    - (ii) all necessary access to such information as may be required by the Supplier in order to render the Service, including but not limited to Customer Data, security access information and configuration services;
  - 9.1.2 comply with all applicable laws and regulations with respect to its activities under this Agreement;
  - 9.1.3 carry out all other Customer responsibilities set out in this Agreement in a timely and efficient manner. In the event of any delays in the Customer's provision of such assistance as agreed by the parties, the Supplier may adjust any agreed timetable or delivery schedule as reasonably necessary;
  - 9.1.4 ensure that the Users use the Service in accordance with the terms and conditions of this Agreement and shall be responsible for any User's breach of this Agreement;
  - 9.1.5 obtain and shall maintain all necessary licenses, consents, and permissions necessary for the Supplier, its contractors and agents to perform their obligations under this Agreement, including without limitation the Service;
  - 9.1.6 ensure that its network and systems comply with the relevant specifications provided by the Supplier from time to time;
  - 9.1.7 shall be solely responsible for protecting and safeguarding all Application Passwords, as Customer will be the only party with knowledge of its passwords. If Customer makes such Application Passwords available to any third party, Customer shall be liable for all actions taken by such third party in connection with the Service. Customer shall not disclose or make available the Application Password other than to Customer's authorized employees or contractors, shall use all commercially reasonable efforts to prevent unauthorized access to, or use of, the Application Password and the Service and will notify the Supplier promptly of any such unauthorized access or use and make any disclosures related to such unauthorized access or use which may be required under any applicable laws; and
  - 9.1.8 be solely responsible for procuring and maintaining its network connections and telecommunications links from its systems to the Supplier, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Customer's network connections or telecommunications links or caused by the internet.

## 10 PROFESSIONAL SERVICES



- 10.1 Customer may retain Supplier to perform Professional Services as the parties may agree upon in writing ("Work Order"). Supplier will use reasonable efforts to carry out the Professional Services stated in the Work Order and to provide any resulting functionality in the Service made available online to Customer and Customer's Users. Except as the parties otherwise agree in a Work Order, Professional Services and the results thereof are made available "AS IS."
- 10.2 Unless otherwise agreed in writing either under this Agreement or in the Work Order, Professional Services are provided by Supplier on a time and materials basis. Maintenance and support of code or functionality created by means of Professional Services will likewise be on a Work Order basis under this clause 10 unless otherwise agreed in writing. The code and functionality made or provided under this clause 10 and all proprietary and intellectual property interests therein, will be Supplier's property. Access to the results of Professional Services will be available, subject to any further terms as may be agreed between the parties, as part of the Service during the Term unless otherwise agreed in writing.

**11 INTELLECTUAL PROPERTY RIGHTS**

- 11.1 Customer will not acquire any title copyright or other proprietary rights or Intellectual Property Rights in the Service or to the source code of the Service including in any materials or supporting documentation provided under the Service as provided in this Agreement.
- 11.2 The Supplier shall at all times be the sole owner of all title and Intellectual Property Rights emanating from any intellectual property, additional coding, data or patents, any discovery, invention, secret process, development, research or improvement in procedure that may be generated in connection with this Agreement including, but not limited to, any derivative works and Customer-specific enhancements and modifications. All intellectual property and other proprietary rights made, conceived or developed by the Supplier alone or in connection with the Customer in the course of the supply of the Service shall at all times be and remain the sole and exclusive property of the Supplier along with any improvement of any process, know-how, technology and any other materials in respect of the Service to be provided under this Agreement.
- 11.3 The Customer agrees not to remove, modify or use in any way any of Supplier's proprietary marking, including any trade mark, product or service names or copyright notice, without the prior written consent of the Supplier.

**12 PRIVACY**

Supplier agrees to implement its privacy policies in effect from time to time.

**13 SERVICE LEVEL WARRANTY**

Supplier warrants during the Term of this Agreement that the Service will meet the Service Level Commitment stated in Schedule 1.

**14 ADDITIONAL WARRANTIES**

Each party represents and warrants that it has the legal power and authority to enter into this Agreement.

**15 INDEMNIFICATION**

- 15.1 Supplier will defend, indemnify, and hold Customer (and its officers, directors, employees and agents) harmless from and against all costs, liabilities, losses, and expenses (including reasonable legal fees) (collectively, "Losses") arising from any third-party claim, suit, action, or proceeding arising from the actual or alleged infringement of any copyright, patent, trademark, or misappropriation of a trade secret by the Service or Supplier Content (other than that due to Customer Data). In case of such a claim, Supplier may, in its discretion, procure a license that will protect Customer against such claim without cost to Customer or replace the Service with a non-infringing Service. THIS CLAUSE 15.1 STATES CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES FOR INFRINGEMENT OR CLAIMS ALLEGING INFRINGEMENT. This indemnity by Supplier shall not apply to the extent that the claim of infringement of Intellectual Property Rights arose as a result of i) any negligent act or omission or willful misconduct of the Customer pursuant to this Agreement; (ii) any misuse or modification of the Service by the Customer, including, but not limited to the Customer's use of the Service in a manner inconsistent with information, directions, specifications, or instructions provided and approved by Supplier; (iii) the Customer's use of the Service in combination or conjunction with any product, service, device, or method not owned, developed, furnished, recommended, or approved by Supplier; (iv) the combination, operation or use of the Service with non-Supplier programs, data, methods or technology if such infringement would have been avoided without the combination, operation or use of the Service with other programs, data, methods or technology, or (v) Customer's breach of any of the provisions of section 7 of this Agreement.
- 15.2 Customer will defend, indemnify, and hold Supplier (and its officers, directors, employees and agents) harmless from and against all Losses arising out of or in connection with a claim, suit, action, or proceeding by a third party (i) alleging that the Customer Data or other data or information supplied by Customer infringes the intellectual property rights or other rights of a third party or has caused harm to a third party or (ii) arising out of breach of clause 7 above.
- 15.3 Customer will defend, indemnify, and hold Supplier (and its officers, directors, employees and agents) harmless from any expense or cost arising from any third-party subpoena or compulsory legal order or process that seeks Customer Data and/or other Customer-related information or data, including, without limitation, prompt payment to Supplier of all costs (including legal fees) incurred by Supplier as a result. In case of such subpoena or compulsory legal order or process, Customer also agrees to pay Supplier for its staff time in responding to such third-party subpoena or compulsory legal order or process at Supplier's then applicable hourly rates.
- 15.4 In case of any claim that is subject to indemnification under this Agreement, the party that is indemnified ("Indemnitee") will provide the indemnifying party ("Indemnitor") reasonably prompt notice of the relevant claim. Indemnitor will defend and/or settle, at its own expense, any demand, action, or suit on any claim subject to indemnification under this Agreement. Each party will cooperate in good faith with the other to facilitate the defense of any such claim and will tender the defense and settlement of any action or proceeding covered by this clause 15 to the Indemnitor upon request. Claims may be settled without the consent of the Indemnitee, unless the settlement includes an admission of wrongdoing, fault or liability.

**16 DISCLAIMERS AND LIMITATIONS**

- 16.1 Except with regard to Customer's payment obligations under clause 5 and with regard to either party's indemnification obligations under clause 15, in no event will either party's aggregate liability exceed the Service Fees due for the preceding 12-month period at the time of the event or circumstance giving rise to such claim. Except in regard to Customer's breach of clause 7, in no event

will either party be liable for any indirect, special, incidental, consequential damages of any type or kind (including, without limitation, loss of data, revenue, profits, use or other economic advantage).

- 16.2** The Supplier is not responsible for any defects or damages resulting from Customer's or Customer's agents or employees mishandling, abuse, misuse, accident or Force Majeure. The Customer agrees to inform the Supplier of any Customer system change that may reasonably be expected to affect the Supplier's ability to provide the Service and shall notify the Supplier of any change to its IT configuration affecting the Services. The Supplier shall not be held responsible for the availability of telephone lines, the Internet, electricity or servers outside its reasonable control. The Supplier provides no warranty or guarantee in relation to speed of delivery of the Service, including the speed of any restores. The speed of delivery of the Service is dependent on factors outside the control of the Supplier including inter alia the speed, functionality and condition of the Customer's IT infrastructure, the amount of data being restored and/or the bandwidth of the Customer's internet connection. Any errors caused arising from the inadequacy or defectiveness of the Customer's IT infrastructure and/or the connectivity and bandwidth of the Customer's internet connection may affect the delivery of the Service including the performance of any restores. The Supplier will notify Customer of any technical failures in respect of delivery of the Service of which it is aware and subject to the terms of the Service Level Commitments, will endeavor to work with Customer to assist with rectification of any such failures. Customer acknowledges that changes may be required to the Customer's IT infrastructure and/or to its internet connectivity including its bandwidth capacity or otherwise to improve the speed, performance and/or delivery of the Service. Customer shall be responsible for the cost of any such changes. Any administrative and technical notifications in respect of the delivery of the Service will be sent by email to the Customer.
- 16.3** Except as set forth in the Service Level Commitments, the Supplier makes no warranty that the Service will be uninterrupted, timely, secure or error free. The Supplier expressly disclaims all liability howsoever arising from any change made to the Customer's IT configuration of the Client Environment of which Customer has not notified the Supplier in writing. No statement, whether oral or written, obtained by Customer from the Supplier shall create any warranty not expressly made herein.
- 16.4** The Customer recognizes that the Internet consists of multiple participating networks that are separately owned and not subject to the Supplier's control. The Customer agrees that the Supplier shall not be liable for damages incurred or sums paid when the Service is temporarily or permanently unavailable due to malfunction of, or cessation of, internet services by networks or Internet service providers not subject to the Supplier's control, or for transmission errors in, corruption of, or the security of the Customer Data or data transmitted through the Service carried on such networks or Internet service providers. The Supplier shall have no liability hereunder for damages incurred or sums paid due to any fault of Customer or any third party, or by any harmful components (such as computer viruses, worms and computer sabotage). The Supplier is not liable for any breach of security on the Customer's network, regardless of whether any remedy provided in this Agreement fails in its essential purpose.
- 16.5** THE WARRANTIES EXPRESSLY STATED IN THIS AGREEMENT ARE THE SOLE AND EXCLUSIVE WARRANTIES OFFERED BY SUPPLIER. THERE ARE NO OTHER WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THOSE OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE SERVICES ARE PROVIDED TO CUSTOMER ON AN "AS IS" AND "AS AVAILABLE" BASIS. CUSTOMER ASSUMES ALL RESPONSIBILITY FOR DETERMINING WHETHER THE SERVICE OR THE INFORMATION GENERATED THEREBY IS ACCURATE OR SUFFICIENT FOR CUSTOMER'S PURPOSES.

## **17 CONFIDENTIALITY**

- 17.1** "Confidential Information" means non-public information, technical data or know-how of a party and/or its Affiliates, which is furnished to the other party in written or tangible form in connection with this Agreement. Oral disclosure will also be deemed Confidential Information if it would reasonably be considered to be of a confidential nature or if it is confirmed at the time of disclosure to be confidential.
- 17.2** Notwithstanding the foregoing, Confidential Information does not include information which is: (i) already in the possession of the receiving party and not subject to a confidentiality obligation to the providing party; (ii) independently developed by the receiving party; (iii) publicly disclosed through no fault of the receiving party; (iv) rightfully received by the receiving party from a third party that is not under any obligation to keep such information confidential; (v) approved for release by written agreement with the disclosing party; or (vi) disclosed pursuant to the requirements of law, regulation, or court order, provided that the receiving party will promptly inform the providing party of any such requirement and cooperate with any attempt to procure a protective order or similar treatment.
- 17.3** Neither party will use the other party's Confidential Information except as reasonably required for the performance of this Agreement. Each party will hold in confidence the other party's Confidential Information by means that are no less restrictive than those used for its own confidential materials. Each party agrees not to disclose the other party's Confidential Information to anyone other than its employees or subcontractors who are bound by confidentiality obligations and who need to know the same to perform such party's obligations hereunder. The confidentiality obligations set forth in this clause 17 will survive for five (5) years after the termination or expiration of this Agreement.
- 17.4** Upon termination or expiration of this Agreement, except as otherwise agreed in writing or otherwise stated in this Agreement, each party will, upon the request of the disclosing party, either: (i) return all of such Confidential Information of the disclosing party and all copies thereof in the receiving party's possession or control to the disclosing party; or (ii) destroy all Confidential Information and all copies thereof in the receiving party's possession or control. The receiving party will then, at the request of the disclosing party, certify in writing that no copies have been retained by the receiving party, its employees or agents.
- 17.5** In case a party receives legal process that demands or requires disclosure of the disclosing party's Confidential Information, such party will give prompt notice to the disclosing party, if legally permissible, to enable the disclosing party to challenge such demand.

## **18 DATA PROTECTION**

- 18.1** The parties agree that the Customer is the Data Controller and the Supplier is the Data Processor in respect of any Personal Data.
- 18.2** The Supplier will:
- 18.2.1** take appropriate technical and organizational measures against unauthorized or unlawful processing of, and accidental loss or destruction of, or damage to, Personal Data, having regard to the state of technological development and the cost of implementing any measures, to ensure a level of security appropriate to the harm that might result from such unauthorized or unlawful processing, accidental loss, destruction or damage and the nature of the Personal Data;

- 18.2.2** only process Personal Data in accordance with instructions from the Customer and the Customer shall not provide the Supplier access to sensitive personal information that imposes specific security data security obligations for the processing of such data.; and
- 18.2.3** take reasonable steps to ensure the reliability of its employees who have access to the Personal Data.

## 19 TERMINATION

### 19.1

- 19.1.1** If a party:
- (a) commits a material breach of this Agreement which cannot be remedied; or
  - (b) commits a material breach of this Agreement which can be remedied but fails to remedy that material breach within sixty (60) days of a written notice setting out the breach and requiring it to be remedied being given by the other party (or such longer period where agreed between the parties.
- the other party may terminate this Agreement immediately by giving not less than sixty (60) days' written notice to that effect to the party in breach.
- 19.1.2** A breach can be remedied if the party in breach can comply with the relevant obligation in all respects other than as to time of performance unless time of performance of such obligation is of the essence.
- 19.1.3** This clause 19.1 will not apply to any failure by the Customer to make any payment due to the Supplier under this Agreement on or before the due date. Clause 19.2 will apply instead to any such failure.
- 19.2** The Supplier may terminate this Agreement by giving not less than thirty (30) days' written notice to that effect to the Customer if the Customer fails to make any payment due to the Supplier under this Agreement within 60 days after the relevant due date for payment.
- 19.3** Either party may terminate this Agreement immediately by giving written notice to that effect to the other party if the other party becomes Insolvent. Each party will notify the other party immediately upon becoming Insolvent.
- 19.4** If an application for an administration order, a notice of intention to appoint an administrator or a winding up petition is the only grounds for giving notice to terminate, that notice will be deemed to be ineffective if:
- 19.4.1** in the event of an application for an administration order being made, that application is withdrawn or dismissed within 10 Business Days of being made;
  - 19.4.2** in the event of a notice of intention to appoint an administrator being filed, no administrator is appointed within 10 Business Days of the notice being filed; or
  - 19.4.3** in the event of a winding up petition being presented, that petition is withdrawn or dismissed prior to advertisement and within 10 Business Days of presentation.
- 19.5** The Supplier's rights of termination set out in this Agreement are in addition to and not in substitution for any rights of termination which may exist at common law.
- 19.6** Termination of this agreement for any reason, shall not affect the accrued rights, remedies, obligations or liabilities of the parties existing at termination.

## 20 CONSEQUENCES OF TERMINATION

- 20.1** The termination of this Agreement howsoever arising is without prejudice to the rights, duties and liabilities of either party accrued prior to termination.
- 20.2** If the Supplier terminates or suspends the Service under this Agreement, Customer must pay within 30 days all Service Fees and Professional Services Fees that have accrued prior to such termination or suspension, as well as any fees that remain unpaid for the Service up to date of termination or suspension plus related taxes and expenses. If the Agreement is terminated by Customer for any reason other than a termination expressly permitted by the Agreement, Customer agrees that the Supplier shall be entitled to the Service Fees payable for the Service under the Agreement for the entire Initial Term or if terminated during an Extended Term, the Service Fees payable for the entire Extended Term, unless a provision to the contrary is stipulated in the Agreement.
- 20.3** The clauses in this Agreement which expressly or impliedly have effect after termination will continue to be enforceable notwithstanding termination.
- 20.4** The Customer shall not be entitled on or after the termination of this Agreement for any reason whatsoever to a rebate of any Service Fees paid in advance of their due date.
- 20.5** On termination of this Agreement howsoever arising the Customer will at the direction of the Supplier return to the Supplier any documents in its possession or control which contain or record any Confidential Information.

## 21 FORCE MAJEURE

- 21.1** Neither party to this Agreement will be deemed to be in breach of this Agreement or otherwise liable to the other party in any manner whatsoever for any failure or delay in performing its obligations under this Agreement due to Force Majeure, provided that it has complied and continues to comply with its obligations set out in clause 21.2.
- 21.2** If a party's performance of its obligations under this Agreement is affected by Force Majeure:
- 21.2.1** it will give written notice to the other party, specifying the nature and extent of the Force Majeure, within seven days of becoming aware of the Force Majeure and will at all times use all reasonable endeavors to bring the Force Majeure event to an end and, whilst the Force Majeure is continuing, to mitigate its severity, without being obliged to incur any expenditure;
  - 21.2.2** subject to the provisions of clause 21.3, the date for performance of such obligation will be deemed suspended only for a period equal to the delay caused by such event;
  - 21.2.3** it will not be entitled to payment from the other party in respect of extra costs and expenses incurred by virtue of the Force Majeure.
- 21.3** If the Force Majeure in question continues for more than three months a party may give written notice to the other to terminate this Agreement. The notice to terminate must specify the termination date, which must not be less than 15 days and once such notice has been validly given, this Agreement will terminate on that termination date.
- 21.4** If the Agreement is terminated in accordance with clause 21.3, then neither party will have any liability to the other except that rights and liabilities which accrued prior to such termination will continue to exist.

**22 EMPLOYEES NON-SOLICITATION**

- 22.1** Notwithstanding any degree of supervision exercised by either party over employees of the other, in no circumstances will the relationship of employer and employee be deemed to arise between either party and an employee of the other.
- 22.2** Unless this Agreement is earlier terminated by reason of the Supplier's Insolvency ("Insolvency Event") when no such restrictions shall apply, during the term of this Agreement and for a period of six months after its termination, Customer will not and will ensure that its Affiliates will not, directly or indirectly, without the prior written consent of the other, solicit, or permit any of its group companies to solicit or entice, the employment of any person who is employed by the other party or any of its group companies and whose role either wholly or partly relates to the provision of the Service or the performance of this Agreement. For the purposes of this clause 22 "solicit" or "entice" means the soliciting or enticing of such person with a view to engaging such person as an employee, director, sub-contractor, consultant or independent contractor or through a company owned by such person or his or her family, but will not apply in the case of any such person responding without enticement to a job advertisement which is capable of being responded to by members of the public (or sections thereof) generally.
- 22.3** In such circumstances where the Supplier suffers an Insolvency Event, nothing in this clause 22 will prohibit the Customer from soliciting or enticing or attempting to solicit or entice the employment of any of the key personnel for the duration of that Insolvency Event.

**23 ASSIGNMENT**

- 23.1** Either party may assign, novate or deal in any other manner with any of its rights and obligations under this Agreement.
- 23.2** Subject to the foregoing, this Agreement will be binding upon, and inure to the benefit of the parties and their respective successors and permitted assigns.

**24 NOTICES**

- 24.1** Notices will be in writing, in the English language, marked for the attention of the specified representative of the party to be given the notice or communication and:
  - 24.1.1** sent by pre-paid first-class post to that party's address;
  - 24.1.2** sent by e-mail to that party's e-mail address (with a copy sent by pre-paid to that party's address within 24 hours after sending the e-mail).The address, e-mail address and representative for each party are set out below and may be changed by that party giving at least 5 Business Days' notice in accordance with this clause 24:

[Redacted]

**Prime Government Solutions**  
220 N. 1200 E. #201  
Lehi, UT 84043

**For the attention of:**

For the attention of: Sherif Agib  
sherif@primegov.com

- 24.2** Any Notice given in accordance with 24.1 will be deemed to have been served:
  - 24.2.1** if given as set out in clause 24.1.1 at 9.00 am on the second Business Days after the date of posting;
  - 24.2.2** if given as set out in clause 24.1.2, at the time of sending (except that if an automatic electronic notification is received by the sender within 24 hours after sending the e-mail informing the sender that the e-mail has not been delivered to the recipient or that the recipient is out of the office, that e-mail will be deemed not to have been served);

**25 RELIANCE ON REPRESENTATIONS**

- 25.1** The Customer acknowledges that this Agreement has not been entered into wholly or partly in reliance on, nor has the Supplier given or made, any warranty, statement, promise or representation other than as expressly set out in this Agreement.
- 25.2** Nothing in this clause 25 will exclude any liability which one party would otherwise have to the other party in respect of any statements made fraudulently.

**26 SET-OFF OR WITHHOLDING**

All payments to be made by the Customer to the Supplier under this Agreement will (in the absence of express written agreement from the Supplier) be made in full without any set-off, restriction or condition and without any deduction or withholding for or on account of any counterclaim or any present or future taxes, levies, duties, charges, fees, deductions or withholdings of any nature unless the Customer is required by law to make any such deduction or withholding and Customer has given prior notification to Supplier of such legal obligations on the Customer's part.

**27 ENFORCEMENT BY THIRD PARTIES**

The terms and conditions of this Agreement are for the sole benefit of the parties and nothing herein will be construed as giving any rights to any person or party not a party to it.

**28 INVALIDITY/SEVERABILITY**

If any clause or part of this Agreement is found by any court, tribunal, administrative body or authority of competent jurisdiction to be illegal, invalid or unenforceable then that provision will, to the extent required, be severed from this Agreement and will be ineffective without, as far as is possible, modifying any other clause or part of this Agreement and this will not affect any other provisions of this Agreement which will remain in full force and effect.

**29 VARIATION**

This Agreement may only be varied or amended in writing and signed by the parties or their authorized representatives of each of the parties.

**30 WAIVER**

No failure or delay by the Supplier to exercise any right, power or remedy will operate as a waiver of it nor will any partial exercise preclude any further exercise of the same, or of some other right, power or remedy.

**31 DISPUTE RESOLUTION**

**31.1** If a dispute arises out of or in connection with this Agreement or the performance, validity or enforceability of it (“Dispute”) then, except as expressly provided in this Agreement, the parties shall follow the dispute resolution procedure set out in this clause 32.

**31.2** The parties will initially seek to resolve the Dispute through discussion and negotiation in good faith between the appropriate officers of the parties. If the Dispute is not resolved, through discussion and negotiation under this section, within thirty (30) days (or such alternative time period as may be agreed between the Parties), the following procedure will apply:-

**31.2.1** Any dispute relating to the terms, interpretation or performance of this Agreement (other than claims for preliminary injunctive relief or other pre-judgment remedies) will be resolved at the request of either party through binding arbitration. Arbitration will be conducted under the rules and procedures of the American Arbitration Association (“AAA”). The parties will request that AAA appoint a single arbitrator. Judgment on the arbitrator’s award may be entered in any court having jurisdiction. In the event any provision of this Agreement is held by a tribunal of competent jurisdiction to be contrary to the law, the remaining provisions of this Agreement will remain in full force and effect and an enforceable provision that most closely reflects the parties’ intent will be substituted for the unenforceable provision. The waiver of any breach or default of this Agreement will not constitute a waiver of any subsequent breach or default, and will not act to amend or negate the rights of the waiving party.

**32 GOVERNING LAW AND JURISDICTION**

**32.1** The formation, existence, construction, performance, validity and all aspects whatsoever of this Agreement or of any term of this Agreement will be governed by the laws of the State of California.

**32.2** The courts of California will have non-exclusive jurisdiction to settle any disputes which may arise out of or in connection with this Agreement. The parties irrevocably agree to submit to that jurisdiction except that either party may seek injunctive relief in any court of competent jurisdiction.

**33 MERGER AND MODIFICATION**

This Agreement, including the attached documents, constitutes the entire agreement between the parties. There are no understandings, agreements, or representations, oral or written, not specified within this Agreement. This Agreement may not be modified, supplemented, or amended, in any manner, except by written agreement signed by both parties.

**34 NONDISCRIMINATION AND COMPLIANCE WITH LAWS**

Supplier agrees to comply with all applicable laws, rules, regulations, and policies, including those relating to nondiscrimination, accessibility, and civil rights. Supplier agrees to timely file all required reports, make required payroll deductions, and timely pay all taxes and premiums owed, including sales and use taxes and unemployment compensation and workers’ compensation premiums. Supplier shall have and keep current at all times during the term of this Agreement all licenses and permits required by law.

**SIGNED BY** the parties on the date stated at the beginning of this Agreement.

**PRIME GOVERNMENT SOLUTIONS LLC**

.....

**CUSTOMER NAME**

.....

**SCHEDULE 1 – Support Services SLA**

The SLA describes the expected performance of the PrimeGov Service, the procedures for reporting an issue and expected turnaround time on issues reported.

**A. Service Uptime Target**

PrimeGov have a target uptime of >99.95% measured on a monthly basis. This time excludes any planned outages that have been identified to the Customer. PrimeGov must give a minimum of two business days notice for a planned outage. Planned outages will be targeted to occur between 00:01 on Saturdays to 23:59 on Sunday night.

**B. Reporting an Issue**

**1. Contact Details**

At PrimeGov we build our Service with alerting to anticipate any Service disruption so that our Customer Success team can address any technical items before they become an issue for our customers. In the case where a Customer discovers a defect or fault, or the Service is unavailable, the Customer should notify the PrimeGov Customer Success team through one of the following channels:

- Enter a ticket in the help desk system at [primegov.freshdesk.com](http://primegov.freshdesk.com)
- E-mail: [support@primegov.com](mailto:support@primegov.com)
- Phone: 801-341-1910

**2. Hours of Coverage**

The Support Services will be provided between Business Days 08:00 to 18.00 MT, from Monday to Friday. More specifically, the hours are as follows:

- Service support 08:00 to 18.00 MT
- Enter an issue in the help desk system This service will be available 24 hours a day – 7 days a week
- Email an issue to the Customer Success team This service will be available 24 hours a day – 7 days a week

**3. Customer Priority Identification**

The Customer will supply their determined priority for each support item logged in accordance with the following Priority Code.

Priority Code	Description
P1	<b>Critical</b> - The problem is impacting all Users by the Service being unavailable with no work around available.
P2	<b>High</b> - The problem is impacting a significant number of Users and is causing a significant business impact, where there is no workaround available.
P3	<b>Moderate</b> - The problem is impacting a small number of Users and is causing a minor business impact or is causing a significant business impact, but there is a workaround available
P4	<b>Low</b> – NON-SERVICE AFFECTING DEFECT –Non-urgent or cosmetic problems, queries, causing inconvenience only.

**C. Resolving an Issue**

**1. Steps to Resolution**

- a) PrimeGov Customer Success staff will analyze the issue and revert to the Customer with an assessment of the issue
- b) The issue will then result in one of the following actions:
  - a. The PrimeGov Customer Success staff will send a set of steps to close the issue with associated times.
  - b. PrimeGov Customer Success staff will ask for more clarification/ information on the issue.
  - c. PrimeGov Customer Success staff may discuss the priority of the issue.
- c) The Customer and the PrimeGov Customer Success staff will mutually agree to close or reprioritize an issue.
- d) If a support issue is closed because it has been successfully resolved, then PrimeGov Customer Success staff will provide a brief description of the final solution to the Customer.
- e) If a support issue is closed but it has not been successfully resolved, then PrimeGov Customer Success staff will provide a brief description of the reason for closing the issue to the Customer.

**2. Target Response Time**

PrimeGov will aim to provide the Customer with a response within a specific time limit based on the agreed Priority Code of the Support Issue (a "Target Response Time"). The following Target Response Times are within the Hours of Coverage.

Priority Code	Description	Target Response Time <
P1	Critical	30 Minutes
P2	High	1 Hour
P3	Moderate	2 Hours
P4	Low	40 Hours

**3. Problem Escalation**

A Support Call's Priority Code may be escalated by either the Customer or PrimeGov, if it is found to be more business critical than first realized or if the steps to resolve are proving unsatisfactory. In the event of escalation the following contacts from PrimeGov should be called:

Role	Name	Contact Details
V.P. Customer Success	Larry Thorpe	Larry.thorpe@primegov.com
Director	Josh Hurni	josh.hurni@primegov.com
COO	Sherif Agib	sherif@primegov.com

**4. Minor Enhancements**

Requests by the Customer for minor enhancements or changes to the Service not relating to a defect or error inherent in the Service will be considered on a case by case basis and will be included under this Agreement at the sole discretion of PrimeGov if in the PrimeGov software product roadmap.

**5. Exclusions**

- a) Requests by the Customer for significant enhancements or changes to the Service not relating to a defect or error inherent in the Service will be excluded from this Agreement and will be managed separately.
- b) PrimeGov is only obliged to provide the Support Services with respect to the then current version of the Service. If PrimeGov provides Support Services for older versions/releases, this is done without obligation on an “as-is” basis at PrimeGov’s sole discretion and without any service level applying and PrimeGov may make the provision of further Support Services for older versions of the Service subject to the payment of additional fees.
- c) any alteration, modification or maintenance of the Service by the Customer or any third party which has not been authorized in writing by PrimeGov;
- d) any failure by the Customer to implement any recommendations, solutions to faults, problems or updates previously advised or delivered by PrimeGov to the Customer;
- e) either Party being subject to Force Majeure;
- f) the Customer’s failure, inability or refusal to allow PrimeGov’s personnel proper and uninterrupted access to the Service.