Amendment No. Three to

MA-017-25011394
Between
County of Orange
And
Carahsoft Technology Corp
For
Email Subscription Management Services (GovDelivery)

This AMENDMENT No. Three to Contract MA-017-25011394 (hereinafter referred to as "Amendment No. Three") 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 ("County") and Carahsoft Technology Corp, ("Contractor"), with County and Contractor sometimes individually referred to as "Party" or collectively referred to as "Parties".

Recitals

WHEREAS, County of Orange, County Procurement Office, ("CPO") has issued a Regional Cooperative Agreement RCA-017-25010020, for Software Solutions and Services ("RCA"), effective February 24, 2025, through December 31, 2027, now in effect; and,

WHEREAS, County and Contractor entered into Subordinate Contract MA-017-25011394, per the terms and conditions of the RCA and Contractor's quote #44313471, effective Thursday, May 1, 2025, through Thursday, April 30, 2026, in the amount of $153,530.86 ("Contract"); and,

WHEREAS, the Parties entered into Amendment No.1 to add Volume Overages to Contract per Contractor's quote #55778002, dated May 5, 2025, in an additional amount of $17,700 for a new Total Contract Amount of $171,230.86; and,

WHEREAS, the Parties entered into Amendment No.2 to replace Attachment A, Scope of Work, in its entirety; and

WHEREAS, the Parties now desire to Renew the Contract for one (1) year, effective May 1, 2026, through April 30, 2027, in the amount of $188,023.95 per Contractor's quote #59797858, with a new cumulative contract total of $340,114.81, and incorporate Attachment D. Additional Terms and Conditions – Information Technology, Attachment, E. County IT Security Provisions, Attachment F. County of Orange Security Guidelines, Attachment G. Business Associate Agreement, replace previous Quote #44313471 with Quote #59797858 which includes Granicus Master Subscription Licensing Agreement and incorporate as Exhibit 1. and add Granicus Service Level Requirements as Exhibit 2. to the Contract; and,

NOW THEREFORE, the Parties agree as follows:

1. "Term of Subordinate Agreement" of the Contract shall be amended to include the following:

Contract shall be renewed for one (1) year, effective May 1, 2026, through April 30, 2027, unless otherwise terminated as provided herein.

2. "Compensation & Payment" of the Contract shall be to amended to include the following:

Contractor agrees to provide the email subscription management services at a fixed annual rate, as specified in Exhibit 1 of the Contract.

3. "Notices" of the Contract shall be amended to update the contact information for County as follows:

County: County of Orange
County Executive Office/Communications
Attn: Molly Nichelson
400 W. Civic Center Drive
Santa Ana, CA 92701
Phone: (714) 834-7218
Email: Molly.Nichelson@ceo.oc.gov

County of Orange
County Executive Office, County Procurement Office
Attn: Christina Rojas
400 W. Civic Center Drive
Santa Ana, CA 92701
Phone: (714) 567-7368
Email: Christina.Rojas@ceo.oc.gov

4. Attachment D. Additional Terms and Conditions – Information Technology is hereby incorporated into the Contract and attached hereto for reference.

5. Attachment E. County IT Security Provisions is hereby incorporated into the Contract and attached hereto.

6. Attachment F. County of Orange Security Guidelines is hereby incorporated into the Contract and attached hereto.

7. Attachment G. Business Associate Agreement is hereby incorporated into the Contract and attached hereto.

8. Contractor's quote #59797858 and Granicus Master Subscription Licensing Agreement is attached as Exhibit 1 and is hereby incorporated by reference, except that (1) neither party shall be entitled to attorney's fees pursuant to Section 9.6 of the Granicus Master Subscription Agreement, and (2) Section 4.2 of the End User License Agreement attached to Contractor's quote #59797858 shall include the following: "or (vii) is required for disclosure pursuant to applicable law or court order."

9. Granicus Service Level Requirements are attached as Exhibit 2 and is hereby incorporated by reference.

10. All other terms and conditions in this Contract shall remain unchanged and with full force and effect.

SIGNATURE PAGE

IN WITNESS WHEREOF, the Parties hereto have executed this Amendment on the date first above written.

CARAHSOFT TECHNOLOGY CORP

If the Contractor is a corporation, signatures of two specific corporate officers are required as further set forth.

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

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

DocuSigned by: Robert Moore A8FDBA7CEA5A4BC...	Robert Moore	Vice President	5/20/2026
Signature	Name	Title	Date
Signature	Name	Title	Date

COUNTY OF ORANGE, a political subdivision of the State of California

COUNTY AUTHORIZED SIGNATURE:

		Deputy Procurement Agent	
Signature	Name	Title	Date

APPROVED AS TO FORM:
COUNTY COUNSEL:

Signed by: Mark A. Batarse 98A83B6DE25A437...	Mark A. Batarse	Deputy	5/26/2026
Signature	Name	Title	Date

ATTACHMENT D

ADDITIONAL TERMS AND CONDITIONS - INFORMATION TECHNOLOGY

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, a revocable, royalty-free, non-exclusive, license to use all Software of any type provided by Contractor to County.

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.

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 subject to Contractor's Service Level Agreement and 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.

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 rights, title, and interest in, and all Intellectual Property Rights in and to, all County Data.

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.

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 Exhibit 2. 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.

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.

SERVICE LEVEL FEE REDUCTIONS

Failure by the Contractor to meet the application performance and service level guarantees related to Unscheduled Downtime may result in Outage Credits as set forth in the Service Level Agreement.

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.

TRANS-BORDER DATA FLOWS

Contractor shall not transfer any County Data across a country border.

Attachment E

County of Orange Information Technology Security Provisions

All Contractors with access to County data and/or systems shall establish and maintain policies, procedures, and technical, physical, and administrative safeguards designed to (i) ensure the confidentiality, integrity, and availability of all County data and any other confidential information that the Contractor receives, stores, maintains, processes, transmits, or otherwise accesses in connection with the provision of the contracted services, (ii) protect against any threats or hazards to the security or integrity of County data, systems, or other confidential information, (iii) protect against unauthorized access, use, or disclosure of personal or County confidential information, (iv) maintain reasonable procedures to prevent, detect, respond, and provide notification to the County regarding any internal or external security breaches, (v) ensure the return or appropriate disposal of personal information or other confidential information upon contract conclusion (or per retention standards set forth in the contract), and (vi) ensure that any subcontractor(s)/agent(s) that receives, stores, maintains, processes, transmits, or otherwise accesses County data and/or system(s) is in compliance with statements and the provisions of statements and services herein.

1. This County of Orange Information Technology Security Provisions document provides a high-level guide for contractors to understand the resiliency and cybersecurity expectations of the County. The County of Orange Security Guidelines follow the latest National Institute of Standards and Technology (NIST) 800-53 framework to ensure the highest levels of operational resiliency and cybersecurity.

   Contractor, Contractor personnel, Contractor's subcontractors, any person performing work on behalf of Contractor, and all other agents and representatives of Contractor will, at all times, comply with and abide by all County of Orange Information Technology Security Provisions ("Security Provisions") that pertain to Contractor(s) in connection with the Services performed by Contractor(s) as set forth in the scope of work of this Contract. Any violations of the Security Provisions shall, in addition to all other available rights and remedies available to County, be cause for immediate termination of this Contract. Such Security Provisions include, but are not limited to, County of Orange Information Technology Security Guidelines and Business Associate Contract, as applicable.

   Contractor shall use industry best practices and methods with regard to confidentiality, integrity, availability, and the prevention, detection, response, and elimination of threat, by all appropriate means, of fraud, abuse, and other inappropriate or unauthorized access to County data and/or system(s) accessed in the performance of Services under this Contract.

2. Contractor shall implement and maintain a written information security program that contains reasonable and appropriate security measures designed to safeguard the confidentiality, integrity, availability, and resiliency of County data and/or system(s). The Contractor shall review and update its information security program in accordance with contractual, legal, and regulatory requirements. Contractor shall provide County information about the organization's information security program and/or policies in the form of a security questionnaire.

3. Information Access: Contractor shall use appropriate safeguards and security measures to ensure the confidentiality and security of all County data.

   County may require all Contractor personnel, subcontractors, and affiliates approved by County to perform work under this Contract to execute a confidentiality and non-disclosure agreement concerning access protection and data security in the form provided by County. County shall authorize, and

Contractor shall issue, any necessary information-access mechanisms, including access IDs and passwords, and in no event shall Contractor permit any such mechanisms to be shared or used by other than the individual Contractor personnel, subcontractor, or affiliate to whom issued. Contractor shall provide each Contractor personnel, subcontractors, or affiliates with only such level of access as is required for such individual to perform his or her assigned tasks and functions.

Throughout the Contract term, upon request from County, Contractor shall provide County with an accurate, up-to-date list of those Contractor personnel and/or subcontractor personnel having access to County systems and/or County data, and the respective security level or clearance assigned to each such Contractor personnel and/or subcontractor personnel. County reserves the right to require the removal and replacement of Contractor personnel and/or subcontractor personnel at the County's sole discretion. Removal and replacement shall be performed within 14 calendar days of notification by the County.

All County resources (including County systems), County data, County hardware, and County software used or accessed by Contractor: (a) shall be used and accessed by such Contractor and/or subcontractors personnel solely and exclusively in the performance of their assigned duties in connection with, and in furtherance of, the performance of 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 Contractor or Contractor's personnel and subcontractors, at any time.

Contractor acknowledges and agrees that any failure to comply with the provisions of this paragraph shall constitute a breach of this Contract and entitle County to deny or restrict the rights of such non-complying Contractor personnel and/or subcontractor personnel to access and use the County data and/or system(s), as County in its sole discretion shall deem appropriate.

4. Data Security Requirements: Without limiting Contractor's obligation of confidentiality as further described in this Contract, Contractor must establish, maintain, and enforce a data privacy program and an information and cyber security program, including safety, physical, and technical security and resiliency policies and procedures, that comply with the requirements set forth in this Contract and, to the extent such programs are consistent with and not less protective than the requirements set forth in this Contract and are at least equal to applicable best industry practices and standards (NIST 800-53).

   Contractor also shall provide technical and organizational safeguards against accidental, unlawful, or unauthorized access 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.

   Contractor personnel and/or subcontractor personnel and affiliates approved by County to perform work under this Contract may use or disclose County personal and confidential information only as permitted in this Contract. Any other use or disclosure requires express approval in writing by the County of Orange. No Contractor personnel and/or subcontractor personnel or affiliate shall duplicate, disseminate, market, sell, or disclose County personal and confidential information except as allowed in this Contract. Contractor personnel and/or subcontractor personnel or affiliate who access, disclose, market, sell, or use County personal and confidential information in a manner or for a purpose not authorized by this Contract may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

   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 and cyber 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 and cyber security program prior to commencement of Services and from time to time during the term of this Contract. Such review will be in the form of a security questionnaire.

All data belongs to the County and shall be destroyed or returned at the end of the contract via digital wiping, degaussing, or physical shredding as directed by County.

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

6. General Security Standards: Contractor will be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems, email systems, auditing, and monitoring systems) and networks used by or for Contractor ("Contractor Systems") to access County resources (including County systems), County data or otherwise in connection with the Services and shall prevent unauthorized access to County resources (including County systems) or County data through the Contractor Systems.

    a) Contractor System(s) and Security: At all times during the contract term, Contractor shall maintain a level of security with regard to the Contractor Systems, that in all events is at least as secure as the levels of security that are common and prevalent in the industry and in accordance with industry best practices (NIST 800-53). Contractor shall maintain all appropriate administrative, physical, technical, and procedural safeguards to secure County data from data breach, protect County data and the Services from loss, corruption, unauthorized disclosure, and from hacks, and the introduction of viruses, disabling devices, malware, and other forms of malicious and inadvertent acts that can disrupt County's access and use of County data and the Services.

    b) Contractor and the use of Email: Contractor, including Contractor's employees and subcontractors, that are provided a County email address must only use the County email system for correspondence of County business. Contractor, including Contractor's employees and subcontractors, must not access or use personal, non-County Internet (external) email systems from County networks and/or County computing devices. If at any time Contractor's performance under this Contract requires such access or use, Contractor must submit a written request to County with justification for access or use of personal, non-County Internet (external) email systems from County networks and/or computing devices and obtain County's express prior written approval.

Contractors who are not provided with a County email address, but need to transmit County data will be required to maintain and transmit County data in accordance with this Agreement.

7. Security Failures: Any failure by the Contractor to meet the requirements of this Contract with respect to the security of County data, including any related backup, disaster recovery, or other policies, practices or procedures, and any breach or violation by Contractor or its subcontractors or affiliates, or their employees or agents, of any of the foregoing, shall be deemed a material breach of this Contract and may result in termination and reimbursement to County of any fees prepaid by County prorated to the date of such termination. The remedy provided in this paragraph shall not be exclusive and is in addition to any other rights and remedies provided by law or under the Contract.

8. Security Breach Notification: In the event Contractor confirms 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, availability, confidentiality, and/or integrity of County data or the physical, technical, administrative, or organizational safeguards required under this Contract that relate to the security, availability, confidentiality, and/or integrity of County data, Contractor shall, at its own expense, (1) immediately (or within 24 hours confirmed breach), notify the County's Chief Information Security Officer and County Privacy Officer of such occurrence; (2) perform a root cause analysis of the actual, potential, or suspected breach; (3) provide a remediation plan that is acceptable to County within 30 days of verified breach, to address the occurrence of the breach 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, forensics, investigative evidence, 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 officials, 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 reimburse County for all notification and related costs 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.

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

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

   Notification shall be sent to:

Andrew Alipanah, MBA, CISSP
Chief Information Security Officer
721 S. Parker St.
Suite 200
Orange, CA 92868
Phone: (714) 567-7611
Andrew.Alipanah@ocit.oc.gov

Linda Le, CHPC, CHC, CHP
County Privacy Officer
721 S. Parker St.
Suite 200
Orange, CA 92868
Phone: (714) 834-4082
Linda.Le@ocit.oc.gov

9. Security Audits: Contractor shall maintain complete and accurate records relating to its system and Organization Controls (SOC) Type II audits or equivalent's data protection practices, internal and external audits, and the security of any of County-hosted content, including any confidentiality, integrity, and availability operations (data hosting, backup, disaster recovery, external dependencies management, vulnerability testing, penetration testing, patching, or other related policies, practices, standards, or procedures).

   Contractor will provide a copy of its most recent SOC 2 Type 2 audit report to County within thirty (30) days after Contractor's receipt of request for such report(s).

10. County reserves the right, at its sole discretion, to immediately terminate this Contract or a part thereof without limitation and without liability to County if County reasonably determines Contractor fails or has failed to meet its obligations under this section. Business Continuity and Disaster Recovery (BCDR):

    For the purposes of this section, "Recovery Point Objectives" means the maximum age of files (data and system configurations) that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure (establishing the data backup schedule and strategy). "Recovery Time Objectives" means the maximum duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a loss of functionality.

    The Contractor shall maintain a comprehensive risk management program focused on managing risks to County operations and data, including mitigation of the likelihood and impact of an adverse event occurring that would negatively affect contracted services and operations of the County. Business continuity management will enable the Contractor to identify and minimize disruptive risks and restore and recover hosted County business-critical services and/or data within the agreed terms following an adverse event or other major business disruptions. Recovery and timeframes may be impacted when events or disruptions are related to dependencies on third-parties. Granicus Communications has a Recovery Time Objective (RTO) of 90 minutes and a Recovery Point Objective (RPO) of 5 minutes.

    All data and/or systems and technology provided by the Contractor internally and through third-party vendors shall have resiliency and redundancy capabilities to achieve high availability and data recoverability. Contractor Systems shall be designed, where practical and possible, to ensure continuity of service(s) in the event of a disruption or outage.

County of Orange

Information Technology Security Guidelines

All contractors who contract with the County of Orange ("County") shall work cooperatively to assist County in achieving the objectives and abide by the applicable terms under these Guidelines for all Controls one (1) thru six (6) below at all times during the term of its contract with County.

1 ASSET MANAGEMENT

Asset management establishes an organization's inventory of fixed and controlled assets and defines how these assets are managed during their lifecycle to ensure sustained productivity in support of the organization's critical services. An event that disrupts an asset can inhibit the organization from achieving its mission. An asset management program helps identify appropriate strategies that shall allow the assets to maintain productivity during disruptive events. There are four broad categories of assets: people, information, technology, and facilities.

The Cybersecurity Program strives to achieve and maintain appropriate protection of IT assets. Loss of accountability of IT assets could result in a compromise or breach of IT systems and/or a compromise or breach of sensitive or privacy data.

1.1 GOALS AND OBJECTIVES

1.1.1 Services are identified and prioritized.

1.1.2 Assets are inventoried, and the authority and responsibility for these assets is established.

1.1.3 The relationship between assets and the services they support is established.

1.1.4 The asset inventory is managed.

1.1.5 Access to assets is managed.

1.1.6 Information assets are categorized and managed to ensure the sustainment and protection of the critical service.

1.1.7 Facility assets supporting the critical service are prioritized and managed.

1.2 ASSET MANAGEMENT POLICY STATEMENTS

1.2.1 Services Inventory

1.2.1.1 Departments and/or contractors shall maintain an inventory of its services. This listing shall be used by the department and/or contractors to assist with its risk management analysis.

1.2.2 Asset Inventory – Information

1.2.2.1 All information that is created or used within the County's trusted environment in support of County business activities shall be considered the property of the County. All County property shall be used in compliance with this guideline.

1.2.2.2 County information is a valuable asset and shall be protected from unauthorized disclosure, modification, or destruction. Prudent information security standards and practices shall be implemented to ensure that the integrity, confidentiality, and availability of County information are not compromised. All County information shall be protected from the time of its creation through its useful life and authorized disposal.

1.2.2.3 Departments and/or contractors shall establish internal procedures for the secure handling

and storage of all electronically maintained County information that is owned or controlled by the department.

1.2.3 Asset Inventory - Technology (Devices, Software)

1.2.3.1 Departments and/or contractors shall maintain an inventory of all department and/or contractors managed devices that connect to County network resources or processes, stores, or transmits County data including but not limited to:

- Desktop computers,
- Laptop Computers,
- Tablets (iPads and Android devices),
- Mobile Phones (basic cell phones),
- Smart Phones (iPhones, Blackberry, Windows Phones and Android Phones),
- Servers,
- Storage devices,
- Network switches,
- Routers,
- Firewalls,
- Security Appliances,
- Internet of Things (IoT) devices,
- Printers,
- Scanners,
- Kiosks and Thin clients,
- Mainframe Hardware, and
- VoIP Phones.

1.2.3.2 Asset inventory shall map assets to the services they support.

1.2.3.3 Departments and/or contractors shall adopt a standard naming convention for devices (naming convention to be utilized as devices are serviced or purchased).

1.2.3.4 Each department and/or contractor shall ensure that all software used on County systems and in the execution of County business shall be used legally and in compliance with licensing agreements.

1.2.4 Asset Inventory - Facilities

1.2.4.1 Departments and/or contractors shall maintain an inventory of its facilities. This listing shall be used by the department and/or contractor to assist with its risk management analysis.

1.2.4.2 Departments and/or contractors shall identify the facilities used by its critical services.

1.2.5 Access Controls

1.2.5.1 Departments and/or contractors shall establish a procedure that ensures only users with legitimate business needs to access County IT resources are provided with user accounts.

1.2.5.2 Access to County information systems and information systems data shall be based on each user's access privileges. Access controls shall ensure that even legitimate users cannot access stored information unless they are authorized to do so. Access control should start by denying access to everything, and then explicitly granting access according to the "need to know" principle.

1.2.5.3 Access to County information and County information assets should be based on the principle

of "least privilege," that is, grant no user greater access privileges to the information or assets than County responsibilities demand.

1.2.5.4 The owner of each County system, or their designee, provides written authorization for all internal and external user access.

1.2.5.5 All access to internal County computer systems shall be controlled by an authentication method involving a minimum of a user identifier ("ID") and password combination that provides verification of the user's identity.

1.2.5.6 All County workforce members, including contractors, are to be assigned a unique user ID to access the network as applicable.

1.2.5.7 A user account shall be explicitly assigned to a single, named individual. No group or shared computer accounts are permissible except when necessary and warranted due to legitimate business needs. Such need shall be documented prior to account creation and accounts activated only when necessary.

1.2.5.8 User accounts shall not be shared with others including, but not limited to, someone whose access has been denied or terminated.

1.2.5.9 Departments and/or contractors shall conduct regular reviews of the registered users' access level privileges. System owners shall provide user listings to departments for confirmation of user's access privileges.

1.2.6 Asset Sanitation/Disposal

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

1.2.6.2 Prior to re-deployment, storage media shall be appropriately cleansed to prevent unauthorized exposure of data.

1.2.6.3 Surplus, donation, disposal or destruction of equipment containing storage media shall be appropriately disposed according to the terms of the equipment disposal services contract.

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

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

2 CONTROLS MANAGEMENT

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

This domain focuses on the resilience controls that allow an organization to operate during a time of stress. These resilience controls are implemented in the organization at all levels and require various levels of management and staff to plan, define, analyze, and assess.

2.1 GOALS AND OBJECTIVES

2.1.1 Control objectives are established.

2.1.2 Controls are implemented.

2.1.3 Control designs are analyzed to ensure they satisfy control objectives.

2.1.4 Internal control system is assessed to ensure control objectives are met.

2.2 CONTROL MANAGEMENT POLICY STATEMENTS

2.2.1 Physical and Environmental Security

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

2.2.1.2 Restricted areas within facilities that house sensitive or critical County information systems shall, at a minimum, utilize physical access controls designed to permit access by authorized personnel only.

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

2.2.1.4 Access to any office, computer room, or work area that contains sensitive information shall be physically restricted from unauthorized access.

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

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

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

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

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

2.2.2 Network Segmentation

NOTE: This section is applicable to Departments and/or contractors that manage their own network devices.

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

2.2.2.2 Segment the network into multiple, separate zones based on the devices (servers, workstations, mobile devices, printers, etc.) connected to the network.

2.2.2.3 Create separate network segments (e.g., VLANs) for BYOD (“bring your own device”) systems or other untrusted devices.

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

2.2.3 Mobile Computing Devices

To ensure that Mobile Computing Devices (“MCDs”) do not introduce threats into systems that process or store County information, departments’ and/or contractors’ management shall:

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

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

2.2.3.3 Implement applicable access control requirements in accordance with this guideline, such as the enforcement of a system or device lockout after 15 minutes of inactivity requiring re-entering of a password to unlock.

2.2.3.4 Install an encryption algorithm that meets or exceeds industry recommended encryption standard for any MCD that will be used to store County information.

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

2.2.3.6 Provide security awareness training to County and/or contractor employees that informs MCD users regarding MCD restrictions.

2.2.3.7 Label MCDs with County address and/or phone number so that the device can be returned to the County if recovered.

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

2.2.4 Personally Owned Devices

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

2.2.4.1 The connection of any computing device not owned by the County to a County network (except the Public Wi-Fi provided for public use) or computing device is prohibited unless previously approved.

2.2.4.2 The County authorizes the use of personal devices to access resources that do not traverse the County network directly. Such resources include County’s SaaS applications. Access to some agency specific applications, e.g., applications that are subject to compliance regulations, may require prior approval of the County CISO and the associated Department Head.

2.2.4.3 The County will respect the privacy of a user’s voluntary use of a personally owned devices to access County IT resources.

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

2.2.5 Logon Banners and Warning Notices

2.2.5.1 At the time of network login, the user shall be presented with a login banner.

2.2.5.2 All computer systems that contain or access County information shall display warning banners informing potential users of conditions of use consistent with state and federal laws.

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

2.2.5.4 The banner message shall be placed at the user authentication point for every computer

system that contains or accesses County information. The banner message may be placed on an initial logon screen in situations where the logon provides access to multiple computer systems.

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

- User is accessing a government information system for conditions of use consistent with state and federal information security and privacy protection laws.
- System usage may be monitored, recorded, and subject to audit.
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
- Use of the system indicates consent to monitoring and recording.

2.2.6 Authentication

2.2.6.1 Authenticate user identities at initial connection to County resources.

2.2.6.2 Authentication mechanisms shall be appropriate to the sensitivity of the information contained.

2.2.6.3 Users shall not receive detailed feedback from the authenticating system on failed logon attempts.

2.2.7 Passwords

2.2.7.1 County approved password standards and/or guidelines shall be applied to access County systems. These standards extend to mobile devices and personally owned devices used for work.

2.2.7.2 Passwords are a primary means to control access to systems and shall therefore be selected, used, and managed to protect against unauthorized discovery or usage. Passwords shall satisfy the following complexity rule:

- Passwords will contain a minimum of one (1) upper case letter
- Passwords will contain a minimum of one (1) lower case letter
- Passwords will contain a minimum of one (1) number: 1- 0
- Passwords will contain a minimum of one (1) special character: !,@,#,$,%,^,&,*,(,)
- Password characters will not be sequential (Do not use: ABCD , This is ok: ACDB)
- Passwords characters will not be repeated in a row (Do not use: P@$$S. This is ok: P@S)
- COMPLEX PASSWORD EXAMPLE: P@$SWoRd13
- Passphrases example: The$kyIsBlue2day
- Passwords cannot contain the user's full name or network login

2.2.7.3 Passwords shall have a minimum length of twelve (12) characters.

2.2.7.4 Passwords shall not be reused for twelve (12) iterations.

2.2.7.5 Departments and/or contractors shall require users to change their passwords periodically (e.g., every 90 days at the maximum). Changing passwords more often than 90 days is encouraged.

2.2.7.6 Network and application systems shall be configured to enforce automatic expiration of passwords at regular intervals (e.g., every 90 days at the maximum) when the technology is feasible or available.

2.2.7.7 Newly created accounts shall be assigned a randomly generated password prior to account information being provided to the user.

2.2.7.8 No user shall give his or her password to another person under any circumstances.

Workforce members who suspect that their password has become known by another person shall change their password immediately and report their suspicion to management.

2.2.7.9 Users who have lost or forgotten their passwords shall make any password reset requests themselves without using a proxy (e.g., another County employee) unless approved by management. Prior to processing password change requests, the requester shall be authenticated to the user account in question. (e.g., Verification with user's supervisor or the use of passphrases can be used for this authentication process.) New passwords shall be provided directly and only to the user in question.

2.2.7.10 When technologically feasible, a new or reset password shall be set to expire on its initial use at log on so that the user is required to change the provided password to one known only to them.

2.2.7.11 All passwords are to be treated as sensitive information.

2.2.7.12 User Accounts shall be locked after five (5) consecutive invalid logon attempts within a 24-hour period. The lockout duration shall be at least 30 minutes or until a system administrator enables the user ID after investigation. These features shall be configured as indicated when the technology is feasible or available.

2.2.7.13 All systems containing sensitive information shall not allow users to have multiple concurrent sessions on the same system when the technology is feasible or available.

2.2.8 Inactivity Timeout and Restricted Connection Times

2.2.8.1 Automatic lockouts for system devices, including workstations and mobile computing devices, after no more than 15 minutes of inactivity.

2.2.8.2 Automated screen lockouts shall be used wherever possible using a set time increment (e.g., 15 minutes of non-activity). In situations where it is not possible to automate a lockout, operational procedures shall be implemented to instruct users to lock the terminal or equipment so that unauthorized individuals cannot make use of the system. Once logged on, workforce members shall not leave their computer unattended or available for someone else to use.

2.2.8.3 When deemed necessary, user logins and data communications may be restricted by time and date configurations that limit when connections shall be accepted.

2.2.9 Account Monitoring

2.2.9.1 Access to a County network and its resources shall be strictly controlled, managed, and reviewed to ensure only authorized users gain access based on the privileges granted. (e.g., Kiosks provide physical and public access to County networks. These shall be secured to ensure County resources are not accessed by unauthorized users.)

2.2.9.2 The control mechanisms for all types of access to County IT resources by contractors and customers are to be documented.

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

2.2.9.4 After a longer period, such as 60 days, the account shall be disabled by the system when the technology is feasible or available.

2.2.9.5 On a periodic basis, such as quarterly or at least annually, departments shall require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators shall then determine whether to disable accounts that are not assigned to active employees or contractors.

2.2.10 Administrative Privileges

2.2.10.1 Systems Administrators shall use separate administrative accounts, which are different

from their end user account (required to have an individual end user account), to conduct system administration tasks.

2.2.10.2 Administrative accounts shall only be granted to individuals who have a job requirement to conduct systems administration tasks.

2.2.10.3 Administrative accounts shall be requested in writing and must be approved by the Department Head or designated representative using the County Security Review and Approval Process.

2.2.10.4 Systems Administrator accounts that access County enterprise-wide systems or have enterprise-wide impact shall be approved by the CISO using the County Security Review and Approval Process.

2.2.10.5 Systems Administrators shall use separate administrative accounts to manage Mobile Device Management (MDM) platforms but may use the local user's credentials when configuring a mobile phone or tablet device.

2.2.10.6 All passwords for privileged system-level accounts (e.g., root, enable, OS admin, application administration accounts, etc.) shall comply with Section 2.2.7.2.

2.2.11 Remote Access

2.2.11.1 Departments and/or contractors shall take appropriate steps, including the implementation of appropriate encryption, user authentication, and virus protection measures, to mitigate security risks associated with allowing users to use remote access or mobile computing methods to access County information systems.

2.2.11.2 Remote access privileges shall be granted to County workforce and contractors only for legitimate business needs and with the specific approval of department management.

2.2.11.3 All remote access implementations that utilize the County's trusted network environment and that have not been previously deployed within the County shall be submitted to and reviewed by the County. A memorandum of understanding (MOU) shall be utilized for this submittal and review process. This is required for any Suppliers utilizing remote access to conduct maintenance.

2.2.11.4 Remote sessions shall be terminated after 15 minutes of inactivity requiring the user to authenticate again to access County resources.

2.2.11.5 All remote access infrastructure shall include the capability to monitor and record a detailed audit trail of each remote access attempt.

2.2.11.6 All users of County networks and computer systems are prohibited from connecting and/or activating unauthorized dial-up or broadband modems on workstations, laptops, or other computing devices that are simultaneously connected to any County network.

2.2.11.7 Periodic assessments shall be performed to identify unauthorized remote connections. Results shall be used to address any vulnerabilities and prioritized according to criticality.

2.2.11.8 Users granted remote access to County IT infrastructure shall follow all additional policies, guidelines and standards related to authentication and authorization as if they were connected locally. For example, this applies when mapping to shared network drives.

2.2.11.9 Users attempting to use external remote access shall utilize a County-approved multi-factor authentication process.

2.2.11.10 All remote access implementations that involve non-County infrastructure shall be reviewed and approved by both the department and County. This approval shall be received prior to the start of such implementation.

2.2.11.11 Remote access privileges to County IT resources shall not be given to contractors and

customers unless department management determines that these individuals or organizations have a legitimate business need for such access. If such access is granted, it shall be limited to those privileges and conditions required for the performance of the specified work.

2.2.12 Wireless Access

2.2.12.1 Departments and/or contractors shall take appropriate steps, including the implementation of appropriate encryption, user authentication, device authentication and malware protection measures, to mitigate risks to the security of County data and information systems associated with the use of wireless network access technologies.

2.2.12.2 Only wireless systems that have been evaluated for security by both department management and the County shall be approved for connectivity to County networks.

2.2.12.3 County data that is transmitted over any wireless network shall be protected in accordance with the sensitivity of the information.

2.2.12.4 All access to County networks or resources via unapproved wireless communication technologies is prohibited. This includes wireless systems that may be brought into County facilities by visitors or guests. Employees, contractors, and customers are prohibited from connecting and/or activating wireless connections on any computing device that are simultaneously connected to any County network, either locally or remotely.

2.2.12.5 Each department and/or contractor shall make a regular, routine effort to ensure that unauthorized wireless networks, access points, and/or modems are not installed or configured within its IT environments. Any unauthorized connections described above shall be disabled immediately.

2.2.13 System and Network Operations Management

2.2.13.1 Operating procedures and responsibilities for all County information processing facilities shall be formally authorized, documented, and updated.

2.2.13.2 Departments and/or contractor shall establish controls to ensure the security of the information systems networks that they operate.

2.2.13.3 Operational system documentation for County information systems shall be protected from unauthorized access.

2.2.13.4 System utilities shall be available to only those users who have a business case for accessing the specific utility.

2.2.14 System Monitoring and Logging

2.2.14.1 Systems operational staff shall maintain appropriate log(s) of activities, exceptions and information security events involving County information systems and services.

2.2.14.2 Each department and/or contractor shall maintain a log of all faults involving County information systems and services.

2.2.14.3 Logs shall be protected from unauthorized access or modifications wherever they reside.

2.2.14.4 The clocks of all relevant information processing systems and attributable logs shall be synchronized with an agreed upon accurate time source such as an established Network Time Protocol (NTP) service.

2.2.14.5 Auditing and logging of user activity shall be implemented on all critical County systems that support user access capabilities.

2.2.14.6 Periodic log reviews of user access and privileges shall be performed in order to monitor access of sensitive information.

2.2.15 Malware Defenses

2.2.15.1 Departments shall implement endpoint security on computing devices connected to the County network. Endpoint security may include one or more of the following software: anti-virus, anti- spyware, personal firewall, host-based intrusion detection (IDS), network-based intrusion detection (IDS), intrusion prevention systems (IPS), and whitelisting and blacklisting of applications, web sites, and IP addresses.

2.2.15.2 Special features designed to filter out malicious software contained in either email messages or email attachments shall be implemented on all County email systems.

2.2.15.3 Where feasible, any computing device, including laptops and desktop PCs, that has been connected to a non-County infrastructure (including employee home networks) and subsequently used to connect to the County network shall be verified that it is free from viruses and other forms of malicious software prior to attaining connectivity to the County network.

2.2.16 Data Loss Prevention

2.2.16.1 Departments and/or contractors shall implement Data Loss Prevention (DLP) methods to reduce the risk of data breach related to sensitive information.

2.2.16.2 Departments and/or contractors shall deploy encryption software on mobile devices containing sensitive data.

2.2.17 Data Transfer

2.2.17.1 Agreements shall be implemented for the exchange of information between the County and other entities. As well as between departments.

2.2.17.2 County information accessed via electronic commerce shall have security controls implemented based on the assessed risk.

2.2.18 Encryption

2.2.18.1 The decision to use cryptographic controls and/or data encryption in an application shall be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.

2.2.18.2 The decision to use cryptographic controls and/or data encryption on a hard drive or any removable media/device shall be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.

2.2.18.3 Where appropriate, encryption shall be used to protect confidential application data that is transmitted over open, untrusted networks, such as the Internet.

2.2.18.4 When cryptographic controls are used, procedures addressing the following areas shall be established by each department:

2.2.18.5 Determination of the level of cryptographic controls

2.2.18.6 Key management/distribution steps and responsibilities

2.2.18.7 Encryption keys shall be exchanged only using secure methods of communication.

2.2.19 System Acquisition and Development

2.2.19.1 Departments and/or contractors shall identify all business applications that are used by their users in support of primary business functions. This includes all applications owned and/or managed by the department as well as other business applications that are used by the department but owned and/or managed by other County organizations. All business applications used by a department shall be documented in the department's IT security plan as well as their Business Impact Analysis (BIA) for criticality rating (RTO) and continuity purposes.

2.2.19.2 An application owner shall be designated for each internal department business application.

2.2.19.3 All access controls associated with business applications shall be commensurate with the highest level of data used within the application. These same access controls shall also adhere to the guidelines provided in Section 1.2.5: Access Controls.

2.2.19.4 Security requirements shall be incorporated into the evaluation process for all commercial software products that are intended to be used as the basis for a business application. The security requirements in question shall be based on requirements and standards specified in this guideline.

2.2.19.5 In situations where data needs to be isolated because there would be a conflict of interest data security shall be designed and implemented to ensure that isolation.

Business Requirements

2.2.19.6 The business requirements definition phase of system development shall contain a review to ensure that the system shall adhere to County information security standards.

System Files

2.2.19.7 Operating system files, application software and data shall be secured from unauthorized use or access.

2.2.19.8 Clear-text data that results from testing shall be handled, stored, and disposed of in the same manner and using the same procedures as are used for production data.

2.2.19.9 System tests shall be performed on data that is constructed specifically for that purpose.

2.2.19.10 System testing shall not be performed on operational data unless the necessary safeguards are in place.

2.2.19.11 A combination of technical, procedural and physical safeguards shall be used to protect application source code from unintentional or unauthorized modification or destruction. All County proprietary information, including source code, needs to be protected through appropriate role-based access controls. An example of this is a change control tool that records all changes to source code including new development, updates, and deletions, along with check-in and check-out information.

System Development & Maintenance

2.2.19.12 The development of software for use on County information systems shall have documented change control procedures in place to ensure proper versioning and implementation.

2.2.19.13 When preparing to upgrade any County information systems, including an operating system, on a production computing resource; the process of testing and approving the upgrade shall be completed in advance in order to minimize potential security risks and disruptions to the production environment.

2.2.19.14 Any outside suppliers used for maintenance that are visitors to the facility are to be escorted and monitored while performing maintenance to critical systems. This does not apply to contractors that are assigned to work at the facility.

2.2.19.15 Systems shall be hardened, and logs monitored to ensure the avoidance of the introduction and exploitation of malicious code.

2.2.19.16 All County workforce members, including contractors, shall not create, execute, forward, or introduce computer code designed to self-replicate, damage, or impede the performance of a computer's memory, storage, operating system, or application software.

2.2.19.17 In conjunction with other access control policies, any opportunity for information leakage shall be prevented through good system design practices.

2.2.19.18 Departments and/or contractors are responsible for managing outsourced software development related to department-owned IT systems.

System Requirements

Any system that processes or stores County Information shall:

2.2.19.19 Baseline configuration shall incorporate Principle of Least Privilege and Functionality.

2.2.19.20 Systems shall be deployed where feasible to utilize existing County authentication methods.

2.2.19.21 Session inactivity timeouts shall be implemented for all access into and from County networks.

2.2.19.22 All applications are to have access controls unless specifically designated as a public access resource.

2.2.19.23 Meet the password requirements defined in Section 2.2.7: Passwords.

2.2.19.24 Strictly control access enabling only privileged users or supervisors to override system controls or the capability of bypassing data validation or editing problems.

2.2.19.25 Monitor special privilege access, e.g., administration accounts.

2.2.19.26 Restrict authority to change master files to persons independent of the data processing function.

2.2.19.27 Have access control mechanisms to prevent unauthorized access or changes to data, especially, the server file systems that are connected to the Internet, even behind a firewall.

2.2.19.28 Be capable of routinely monitoring the access to automated systems containing County Information.

2.2.19.29 Log all modifications to the system files.

2.2.19.30 Limit access to system utility programs to necessary individuals with specific designation.

2.2.19.31 Maintain audit logs on a device separate from the system being monitored.

2.2.19.32 Delete or disable all default accounts.

2.2.19.33 Restrict access to server file-system controls to ensure that all changes such as direct write, write access to system areas and software or service changes shall be applied only through the appropriate change control process.

2.2.19.34 Restrict access to server-file-system controls that allow access to other users' files.

2.2.19.35 Ensure that servers containing user credentials shall be physically protected, hardened and monitored to prevent inappropriate use.

2.2.20 Procurement Controls

2.2.20.1 Breach notification requirements clause to be included in new or renewal contracts for systems containing sensitive information.

2.2.20.2 Contractor shall report to the County immediately or within 24 hours when contractor becomes aware of any potential or suspected data breach of contractor's or subcontractor's systems involving County's data.

2.2.20.3 Departments shall review all procurements and renewals for software and equipment (hosted/managed by the contractor) that transmits, stores, or processes sensitive information to

ensure that contractors are aware of and are in compliance with County's cybersecurity policies if applicable. Departments shall obtain documentation supporting the business partners, contractors, or consultants' compliance with County's cybersecurity policies such as:

- SOC 1 Type 2
- SOC 2 Type 2
- Security Certifications (ISO, PCI, etc.)
- FedRAMP certification
- Penetration Test Results

2.2.21 IT Services Provided to Public

2.2.21.1 Public access to County electronic information resources shall provide desired services in accordance with safeguards designed to protect County resources. All County electronic information resources are to be reviewed at least quarterly.

2.2.22 Removable Media

2.2.22.1 When no longer required, the contents of removable media shall be permanently destroyed or rendered unrecoverable in accordance with applicable department, County, state, or federal record disposal and/or retention requirement.

3 CONFIGURATION & CHANGE MANAGEMENT

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

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

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

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

3.1 GOALS AND OBJECTIVES

3.1.1 The lifecycle of assets is managed.

3.1.2 The integrity of technology and information assets is managed.

3.1.3 Asset configuration baselines are established.

3.2 CONFIGURATION & CHANGE MANAGEMENT POLICY STATEMENTS

3.2.1 Changes to all information processing facilities, systems, software, or procedures shall be strictly controlled according to formal change management procedures.

3.2.2 Changes impacting security appliances managed by the County (e.g., security architecture, security appliances, County firewall, Website listings, application listings, email gateway, administrative accounts) shall be reviewed by the County in accordance with the County Security Review and Approval Process.

3.2.3 Only authorized users shall make any changes to system and/or software configuration files.

3.2.4 Only authorized users shall download and/or install operating system software, service-related software (such as web server software), or other software applications on County computer systems/devices without prior written authorization from department IT management. This includes, but is not limited to, free software, computer games and peer-to-peer file sharing software.

3.2.5 Each department and/or contractor shall develop a formal change control procedure that outlines the process to be used for identifying, classifying, approving, implementing, testing, and documenting changes to its IT resources.

3.2.6 Each department and/or contractor shall conduct periodic audits designed to determine if unauthorized software has been installed on any of its computers.

3.2.7 As appropriate, segregation of duties shall be implemented by all County departments to ensure that no single person has control of multiple critical systems and the potential for misusing that control.

3.2.8 Production computing environments shall be separated from development and test computing environments to reduce the risk of one environment adversely affecting another.

3.2.9 System capacity requirements shall be monitored, and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.

3.2.10 System acceptance criteria for all new information systems and system upgrades shall be defined, documented, and utilized to minimize risk of system failure.

4 VULNERABILITY MANAGEMENT

The Vulnerability Management domain focuses on the process by which organizations identify, analyze, and manage vulnerabilities in a critical service's operating environment.

4.1 GOALS AND OBJECTIVES

4.1.1 Preparation for vulnerability analysis and resolution activities is conducted.

4.1.2 A process for identifying and analyzing vulnerabilities is established and maintained.

4.1.3 Exposure to identified vulnerabilities is managed.

4.1.4 The root causes of vulnerabilities are addressed.

4.2 VULNERABILITY MANAGEMENT POLICY STATEMENTS

4.2.1 Departments and/or contractors shall develop and maintain a vulnerability management process as part of its Cybersecurity Program.

5 CYBERSECURITY INCIDENT MANAGEMENT

Information Security Incident Management establishes the policy to be used by each department and/or contractor in planning for, reporting on, and responding to computer security incidents. For these purposes an incident is defined as any irregular or adverse event that occurs on a County system or network. The goal of incident management is to mitigate the impact of a disruptive event. To accomplish this goal, an organization establishes processes that:

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

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

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

5.1 GOALS AND OBJECTIVES

5.1.1 A process for identifying, analyzing, responding to, and learning from incidents is established.

5.1.2 A process for detecting, reporting, triaging, and analyzing events is established.

5.1.3 Incidents are declared and analyzed.

5.1.4 A process for responding to and recovering from incidents is established.

5.1.5 Post-incident lessons learned are translated into improvement strategies.

5.2 CYBERSECURITY INCIDENT MANAGEMENT POLICY STATEMENTS

5.2.1 Cybersecurity incident management procedures shall be established within each department and/or contractor to ensure quick, orderly, and effective responses to security incidents. In the event a department has not established these procedures, the department may adopt the County's Cyber Incident Response Plan. The steps involved in managing a security incident are typically categorized into six stages:

5.2.2 System preparation

5.2.3 Problem identification

5.2.4 Problem containment

5.2.5 Problem eradication

5.2.6 Incident recovery

5.2.7 Lessons learned

5.2.8 The department shall act as the liaison between applicable parties during a cybersecurity incident. The department shall be the department's primary point of contact for all IT security issues.

5.2.9 A designated security contact for all cybersecurity incidents.

5.2.10 Departments and/or contractors shall conduct periodic (at least annually) cybersecurity incident

scenario sessions for personnel associated with the cybersecurity incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the cybersecurity incident handling team.

5.2.11 Departments and/or contractors shall develop and document procedures for reporting cybersecurity incidents. For example, all employees, contractors, and customers of County information systems shall be required to note and report any observed or suspected security weaknesses in systems to management. In the event a department has not established these procedures, the department may adopt the County's Cyber Incident Response Plan.

5.2.12 Each department and/or contractor shall familiarize its employees on the use of its cybersecurity incident reporting procedures.

5.2.13 Contact with local authorities, including law enforcement, shall be conducted through an organized, repeatable process that is both well documented and communicated.

5.2.14 Contact with special interest groups, including media and labor relations, shall be conducted through an organized, repeatable process that is both well documented and communicated.

5.2.15 Where a follow-up action against an entity after a cybersecurity incident shall involve civil or criminal legal action, evidence shall be collected, retained, and presented to conform to the rules for evidence as demanded by the relevant jurisdiction(s). At the Department's discretion, they may obtain the services of qualified external professionals to complete these tasks.

5.2.16 Departments and/or contractors shall report cybersecurity incidents to the County pursuant to the Contract.

6 SERVICE CONTINUITY MANAGEMENT

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

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

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

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

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

Business Continuity is intended to counteract interruptions in business activities and to protect critical business processes from the effects of significant disruptions. Disaster Recovery provides for the restoration of critical County assets, including IT infrastructure and systems, staff, and facilities.

6.1 GOALS AND OBJECTIVES

6.1.1 Service continuity plans for high-value services are developed.

6.1.2 Service continuity plans are reviewed to resolve conflicts between plans.

6.1.3 Service continuity plans are tested to ensure they meet their stated objectives.

6.1.4 Service continuity plans are tested, executed, and reviewed.

6.2 SERVICE CONTINUITY MANAGEMENT POLICY STATEMENTS

6.2.1 Backups of all essential electronically maintained County business data and system configurations shall be routinely created and properly stored to ensure prompt restoration.

6.2.2 Each department and/or contractor shall implement and document a backup approach for ensuring the availability of critical application databases, system configuration files, and/or any other electronic information critical to maintaining normal business operations within the department.

6.2.3 The frequency and extent of backups shall be in accordance with the importance of the information and the acceptable risk as determined by each department.

6.2.4 Departments and/or contractors shall ensure that locations where backup media are stored are safe, secure, and protected from environmental hazards. Access to backup media shall be commensurate with the highest level of information stored and physical access controls shall meet or exceed the physical access controls of the data's source systems.

6.2.5 Backup media shall be labeled and handled in accordance with the highest sensitivity level of the information stored on the media.

6.2.6 Departments and/or contractors shall define and periodically test a formal procedure designed to verify the success of the backup process.

6.2.7 Restoration from backups shall be tested initially once the process is in place and periodically afterwards. Confirmation of business functionality after restoration shall also be tested in conjunction with the backup procedure test.

6.2.8 Departments and/or contractors shall retain backup information only as long as needed to carry out the purpose for which the data was collected, or for the minimum period required by law.

6.2.9 Alternate storage facilities shall be used to ensure confidentiality, integrity and availability of all County systems.

6.2.10 Each department and/or contractor shall develop, periodically update, and regularly test business continuity and disaster recovery plans.

6.2.11 Departments and/or contractors shall review and update their Risk Assessments (RAs) and Business Impact Analyses (BIAs) as necessary, determined by department management (annually is recommended). RAs include department identification of risks that can cause interruptions to business processes along with the probability and impact of such interruptions and the consequences to information security. A BIA establishes the list of processes and systems that the department has deemed critical after performing a risk analysis.

6.2.12 Continuity plans shall be developed and implemented to provide for continuity of business operations in the event that critical IT assets become unavailable. Plans shall provide for the availability of information at the required level and within the established Recovery Time Objective (RTO) and their location, as alternate facilities shall be used to maintain continuity.

6.2.13 Each department and/or contractor shall maintain a comprehensive plan document containing its

business continuity plans. Plans shall be consistent, address information security requirements, and identify priorities for testing and maintenance.

6.2.14 Each department and/or contractor shall define failure prevention protocols to maintain confidentiality, integrity and availability. Departments and/or contractors shall automate failover procedures where applicable and maintain adequate (predictable) levels of ancillary components to meet this provision.

ATTACHMENT G

BUSINESS ASSOCIATE AGREEMENT

GENERAL PROVISIONS AND RECITALS

A. The Parties agree that the terms used, but not otherwise defined below in the section titled "DEFINITIONS," 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.

B. 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 Contract that are described in the definition of "Business Associate" in 45 CFR § 160.103.

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

D. 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 Contract 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.

E. 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.

F. The Parties understand that the HIPAA Privacy and Security rules, as defined below in the section titled "DEFINITIONS," Subparagraphs titled "The HIPAA Privacy Rule" and "The HIPAA Security Rule," 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 Agreement 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 Contract.

DEFINITIONS

A. "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.

B. "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.

1. Breach excludes:

a. 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.

b. 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.

c. 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.

2. 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:

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

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

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

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

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

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

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

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

G. "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).

H. "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.

I. "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.

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

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

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

M. "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.

N. "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.

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

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

Q. "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 - https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

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

OBLIGATIONS AND ACTIVITIES OF CONTRACTOR AS BUSINESS ASSOCIATE:

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

B. Contractor agrees to use appropriate safeguards, as provided for in this Business Associate Agreement and the Contract, 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 Agreement.

C. 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.

D. 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 Agreement.

E. Contractor agrees to report to County promptly any Use or Disclosure of PHI not provided for by this Business Associate Agreement of which Contractor becomes aware. Contractor must report Breaches of Unsecured PHI in accordance with the section titled "BREACH DISCOVERY AND NOTIFICATION" below and as required by 45 CFR § 164.410.

F. 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 Agreement to Contractor with respect to such information.

G. 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.

H. 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.

I. 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.

J. 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.

K. 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 Contract, 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.

L. 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.

M. 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 the section titled "DEFINITIONS," Subparagraph titled "Breach excludes" above.

SECURITY RULE

A. 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.

B. 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 section of this Business Associate Agreement.

C. Contractor shall report to County promptly any Security Incident of which it becomes aware. Contractor shall report Breaches of Unsecured PHI in accordance with the section titled "BREACH DISCOVERY AND NOTIFICATION" below and as required by 45 CFR § 164.410.

BREACH DISCOVERY AND NOTIFICATION

A. 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.

1. 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.

2. 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.

B. Contractor shall provide the notification of the Breach promptly to the County Privacy Officer listed below. Contractor's notification may be oral, but shall be followed by written notification within 24 hours of the oral notification.

Andrew Alipanah, MBA, CISSP
Chief Information Security Officer
721 S. Parker Street
Suite 200
Orange, CA 92868

(714) 567-7611
Andrew.Alipanah@ocit.ocgov.com

Linda Le, CHPC, CHC, CHP
County Privacy Officer
721 S. Parker Street
Suite 200
Orange, CA 92868
(714) 834-4082
Linda.Le@ocit.ocgov.com

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

1. 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;

2. 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:

a. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

b. 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);

c. Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;

d. 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

e. 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.

D. 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.

E. 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 section 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.

F. 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.

G. Contractor shall provide to County all specific and pertinent information about the Breach, including the information listed in Section C.3.b.(a)-(e) above of the "BREACH DISCOVERY AND NOTIFICATION", 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 "B" above.

H. 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.

I. 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.

PERMITTED USES AND DISCLOSURES BY CONTRACTOR

A. 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.

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

2. 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:

   a. The Disclosure is required by law; or

   b. 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.

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

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

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

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

OBLIGATIONS OF COUNTY

A. 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.

B. 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.

C. 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.

D. 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.

BUSINESS ASSOCIATE TERMINATION

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

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

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

B. Upon termination of the Contract, 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.

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

   2. Contractor shall retain no copies of the PHI.

   3. 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 Agreement 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.

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

EXHIBIT 1

GOVERNMENT- PRICE QUOTATION

Granicus at Carahsoft

carahsoft.

11493 SUNSET HILLS ROAD | SUITE 100 | RESTON, VIRGINIA 20190
PHONE (703) 871-8500 | FAX (703) 871-8505 | TOLL FREE (888) 66CARAH
WWW.CARAHSOFT.COM | GRANICUS@CARAHSOFT.COM

GRANICUS

TO: Rick Tran
County Executive Procurement/ Contracts Manager
Orange County HCA
400 W Civic Center Dr
2ND FL
Santa Ana, CA 92701 USA

EMAIL: rick.tran@ocgov.com

PHONE: (714) 834-7025

FROM: Mandi Queen
Granicus at Carahsoft
11493 Sunset Hills Road
Suite 100
Reston, Virginia 20190

EMAIL: Mandi.Queen@carahsoft.com

PHONE: (571) 662-3051 **FAX:** (703) 871-8505

TERMS:
FTIN: 52-2189693
Shipping Point: FOB Destination
Remit To: Same as Above
Payment Terms: Net 30 (On Approved Credit)
Cage Code: 1P3C5
DUNS No: 088365767
UEI: DT8KJHZXVJH5
Credit Cards: VISA/MasterCard/AMEX
Sales Tax May Apply

QUOTE NO:	59797858
QUOTE DATE:	02/23/2026
QUOTE EXPIRES:	05/29/2026
RFQ NO:	
SHIPPING:	ESD
TOTAL PRICE:	$188,023.95
TOTAL QUOTE:	$188,023.95

LINE NO.	PART NO.	DESCRIPTION	-	QUOTE PRICE		QTY	EXTENDED PRICE
		RENEWING SUBSCRIPTION FEES					
1	SAS-SB-CO-CC-R-003290-1	Granicus - Communications Cloud (Potential Users 4000000-4999999) Each - Annual Subscription Granicus - SAS-SB-CO-CC-R-003290 Start Date: 05/01/2026 End Date: 04/30/2027		$168,883.95	OM	1	$168,883.95
2	GR-S-SB-CO-SMS	Granicus - SMS (Priced per SMS) - Each - Annual Subscription Communications Cloud SMS Volume Granicus - SAS-SB-CO-SMS Start Date: 05/01/2026 End Date: 04/30/2027		$0.0319	OM	600,000	$19,140.00
		RENEWING SUBSCRIPTION FEES SUBTOTAL:					$188,023.95
		SUBTOTAL:					$188,023.95
			TOTAL PRICE:				**$188,023.95**
			TOTAL QUOTE:				**$188,023.95**

By issuing a Purchase Order against this quote, customer agrees to the Granicus Master Subscription Agreement at the link below:
https://granicus.com/legal-licensing/

For govDelivery Customers Only:
Potential Users are based on the greater of quarterly website visits to the domains covered by a license or the subscriber base multiplied by 12, less 20% to account for inactive subscribers.

Option year pricing is provided with the assumption that your requirements are the same as the base year. If your usage increases Granicus reserves the right to renegotiate your contract based on usage. Option year pricing does not imply usage can grow beyond your base level.

GRANICUS

THIS IS NOT AN INVOICE

Order Form
Prepared for
Orange County CA

Granicus Order Form for Orange County CA

ORDER DETAILS

Granicus Contact:	Tony Bullock
Email:	antonio.bullock@granicus.com
Order #:	Q-508799
Prepared On:	22 Jan 2026

ORDER TERMS

Currency:	USD
Payment Terms:	All fees set forth in the Quote from reseller/distributor to Client are due and payable in accordance with those terms. Use of the Products is governed by the terms of the Granicus Master Subscription Agreement or such other Agreement as agreed to by the parties.
Current Subscription End Date:	30 Apr 2026
Period of Performance:	01 May 2026 - 30 Apr 2027

EXHIBIT 1

GRANICUS

Order Form
Prepared for
Orange County CA

PRODUCT SUMMARY

The specifications and terms within this Order Form are specific to the products and volumes contained herein.

NOTE: Fees for the below Products will be as set forth in the quote from an authorized reseller.

Renewing Subscriptions		
Solution	**Billing Frequency**	**Quantity/Unit**
Communications Cloud	Annual	1 Each

Communications Cloud Tier:
for up to 4,999,999 potential users.

GRANICUS

Order Form
Orange County CA

PRODUCT UPDATES

FOR INFORMATION ON RECENT AND UPCOMING PRODUCT ENHANCEMENTS ACROSS THE GRANICUS PORTFOLIO, PLEASE REFER TO THE SEMIANNUAL UPDATE INFORMATION ON THIS WEBPAGE:
: HTTPS://GRANICUS.COM/SEMIANNUAL-UPDATES/

PRODUCT DESCRIPTIONS

Solution	Description
Communications Cloud	The Cloud is a Software-as-a-Service (SaaS) solution that enables government organizations to connect with more people. By leveraging the Cloud, the client will be able to utilize a number of different outreach mediums, including email, SMS/text messages, RSS feeds, and social media integration to connect with its target audiences. The Cloud includes: • Unlimited email sends with industry-leading delivery and management of all bounces • Support to upload and migrate existing email lists • Access to participate in the govDelivery Network • Ability to send mass notifications to multiple devices • 24/7 system monitoring, email and phone support during business hours, auto-response to inbound messages from end users, and emergency support • Text-to-subscribe functionality • Up to 2 Web-hosted training sessions annually • Up to 50 administrators • Up to 1 govDelivery account(s) • Access to a complete archive of all data created by the client for 18 months (rolling) • Up to 3 hours of message template and integration development • Up to 100 subscription topics • Up to 100,000 SMS/text messages per year* *International numbers are not supported. SMS/text messages not used in the period of performance will not carry over to the following year.

GRANICUS ADVANCED NETWORK AND SUBSCRIBER INFORMATION

- **Granicus Communications Suite Subscriber Information.**
  - Data provided by the Client and contact information gathered through the Client's own web

properties or activities will remain the property of the Client ('Direct Subscriber'), including any and all personally identifiable information (PII). Granicus will not release the data without the express written permission of the Client, unless required by law.

- Granicus shall: (i) not disclose the Client's data except to any third parties as necessary to operate the Granicus Products and Services (provided that the Client hereby grants to Granicus a perpetual, non-cancelable, worldwide, non-exclusive license to utilize any data, on an anonymous or aggregate basis only, that arises from the use of the Granicus Products by the Client, whether disclosed on, subsequent to, or prior to the Effective Date, to improve the functionality of the Granicus Products and any other legitimate business purpose, including the right to sublicense such data to third parties, subject to all legal restrictions regarding the use and disclosure of such information).

- **Data obtained through the Granicus Advanced Network.**
  - Granicus offers a SaaS product, known as the Communications Cloud, that offers Direct Subscribers recommendations to subscribe to other Granicus Client's digital communication (the 'Advanced Network'). When a Direct Subscriber signs up through one of the recommendations of the Advanced Network, that subscriber is a 'Network Subscriber' to the agency it subscribed to through the Advanced Network.
  - Network Subscribers are available for use while the Client is under an active subscription with Granicus. Network Subscribers will not transfer to the Client upon termination of any Granicus Order, SOW, or Exhibit. The Client shall not use or transfer any of the Network Subscribers after termination of its Order, SOW, or Exhibit placed under this agreement. All information related to Network Subscribers must be destroyed by the Client within 15 calendar days of the Order, SOW, or Exhibit placed under this agreement terminating.
  - Opt-In. During the last 10 calendar days of the Client's subscription, the Client may send an opt-in email to Network Subscribers that shall include an explanation of the Client's relationship with Granicus terminating and that the Network Subscribers may visit the Client's website to subscribe to further updates from the Client in the future. Any Network Subscriber that does not opt-in will not be transferred with the subscriber list provided to the Client upon termination.

GRANICUS

TERMS & CONDITIONS

- This quote, and all products and services delivered hereunder are governed by the terms located at https://granicus.com/legal/licensing, including any product-specific terms included therein (the "License Agreement"). If your organization and Granicus has entered into a separate agreement or is utilizing a contract vehicle for this transaction, the terms of the License Agreement are incorporated into such separate agreement or contract vehicle by reference, with any directly conflicting terms and conditions being resolved in favor of the separate agreement or contract vehicle to the extent applicable.
- If submitting a Purchase Order, please include the following language: The pricing, terms and conditions of quote Q-508799 dated 22 Jan 2026 are incorporated into this Purchase Order by reference and shall take precedence over any terms and conditions included in this Purchase Order.
- This quote is exclusive of applicable state, local, and federal taxes, which, if any, will be included in the invoice. It is the responsibility of Orange County CA to provide applicable exemption certificate(s).
- Any lapse in payment may result in suspension of service and will require the payment of a setup fee to reinstate the subscription.

- The attached End User Licensing Agreement must be signed and returned with all necessary order documents.
- Client will be invoiced for use of any product or service measured or capped by volume or amount of usage that exceeds the permitted amount set forth in this Quote at the same cost or rate set forth herein.

EXHIBIT 1

GRANICUS

End User License Agreement

This End User License Agreement ("**Agreement**") is made and entered into as of the latter date of the signatures below (the "Effective Date") by and between Orange County CA ("**Client**") and Granicus, LLC, a Minnesota Limited Liability Company d/b/a Granicus ("**Granicus**"). Client and Granicus may each be referred to herein as "Party" or collectively as "Parties".

Whereas Client has entered into an agreement with a third party to purchase Granicus Products and Services ("**Reseller**"), by accessing the Granicus Products and Services, Client accepts this Agreement. Due to the rapidly changing nature of digital communications, this Agreement may be updated from time to time at Granicus' sole discretion. Notification to Client will be via email or posting to the Granicus website.

1. **Definitions.** In addition to terms defined elsewhere in this Agreement, the following terms shall have the meaning specified:

   "Granicus Products and Services" means the products and services made available to Client pursuant to this Agreement, which may include Granicus products and services accessible for use by Client on a subscription basis ("Software-as-a-Service" or "SaaS"), Granicus professional services, content from any professional services or other required equipment components or other required hardware, as specified in each Order.
   "Order" means a written order, proposal, or purchase document in which Granicus agrees to provide and Client agrees to purchase specific Granicus Products and Services via Reseller.
   "Order Term" means the then-current duration of performance identified on each Order, for which Granicus has committed to provide, and Client has committed to pay for via Reseller, Granicus Products and Services.

2. **Use of Granicus Products and Services and Proprietary Rights**
   - **2.1. Granicus Products and Services.** The Granicus Products and Services are purchased by Client, via a Reseller, as subscriptions during an Order Term specified in each Order.
   - **2.2. Permitted Use.** Subject to the terms and conditions of this Agreement, Granicus hereby grants during each Order Term, and Client hereby accepts, solely for its internal use, a worldwide, revocable, non-exclusive, non-transferrable right to use the Granicus Products and Services to the extent allowed in the relevant Order (collectively the "Permitted Use"). The Permitted Use shall also include the right, subject to the conditions and restrictions set forth herein, to use the Granicus Products and Services up to the levels limited in the applicable Order.
     - **2.2.1. Data Sources.** Data uploaded into Granicus Products and Services must be brought in from Client sources (interactions with end users and opt-in contact lists). Client cannot upload purchased contact information into Granicus Products and Services without Granicus' written permission and professional services support for list cleansing.
     - **2.2.2. Passwords.** Passwords are not transferable to any third party. Client is responsible for keeping all passwords secure and all use of the Granicus Products and Services accessed through Client's passwords.
     - **2.2.3. Content.** Client can only use Granicus Products and Services to share content that is created by and owned by Client and/or content for related organizations provided that it is in support of other organizations but not as a primary communication vehicle for other organizations that do not have a Granicus subscription. Any content deemed inappropriate for a public audience or in

support of programs or topics that are unrelated to Client, can be removed or limited by Granicus.

2.2.3.1. **Disclaimers.** Any text, data, graphics, or any other material displayed or published on Client's website must be free from violation of or infringement of copyright, trademark, service mark, patent, trade secret, statutory, common law or proprietary or intellectual property rights of others. Granicus is not responsible for content migrated by Client or any third party.

2.2.4. **Advertising.** Granicus Products and Services shall not be used to promote products or services available for sale through Client or any third party unless approved in writing, in advance, by Granicus. Granicus reserves the right to request and review the details of any agreement between Client and a third party that compensates Client for the right to have information included in Content distributed or made available through Granicus Products and Services prior to approving the presence of Advertising within Granicus Products and Services.

2.2.5. **Granicus Subscriber Information for Communications Cloud Suite only**

2.2.5.1. **Data Provided by Client.** Data provided by Client and contact information gathered through Client's own web properties or activities will remain the property of Client ("Direct Subscriber"), including any and all personally identifiable information (PII). Granicus will not release the data without the express written permission of Client, unless required by law.

2.2.5.2. Granicus shall not disclose the client's data except to any third parties as necessary to operate the Granicus Products and Services (provided that the client hereby grants to Granicus a perpetual, noncancelable, worldwide, non-exclusive license to utilize any data, on an anonymous or aggregate basis only, that arises from the use of the Granicus Products and Services by the client, whether disclosed on, subsequent to, or prior to the Effective Date, to improve the functionality of the Granicus Products and Services and any other legitimate business purpose including the right to sublicense such data to third parties, subject to all legal restrictions regarding the use and disclosure of such information).

2.2.5.3. **Data Obtained through the Granicus Advanced Network**

2.2.5.3.1. Granicus offers a SaaS product, known as the Communications Cloud, that offers Direct Subscribers recommendations to subscribe to other Granicus Client's digital communication (the "Advanced Network"). When a Direct Subscriber signs up through one of the recommendations of the Advanced Network, that subscriber is a "Network Subscriber" to the agency it subscribed to through the Advanced Network.

2.2.5.3.2. Access to the Advanced Network is a benefit of the GovDelivery Communications Cloud subscription with Granicus. Network Subscribers are available for use only on the GovDelivery Communications Cloud while Client is under an active GovDelivery Communications Cloud subscription. Network Subscribers will not transfer to Client upon termination of any Granicus Order, SOW or Exhibit. Client shall not use or transfer any of the Network Subscribers after termination of its Order, SOW or Exhibit placed under this Agreement. All information related to Network Subscribers must be destroyed by Client within 15 calendar days of the Order, SOW or Exhibit placed under this Agreement terminating.

2.2.5.3.3. **Opt-In.** During the last 10 calendar days of Client's Order Term for the terminating Order, SOW or Exhibit placed under this Agreement, Client may send an opt-in email to Network Subscribers that shall include an explanation of Client's relationship with Granicus terminating and that the Network Subscribers may visit Client's website to subscribe to further updates from Client in the future. Any Network Subscriber that does not opt-in will not be transferred with the subscriber list provided to Client upon termination.

2.3. Restrictions. Client shall not:

2.3.1. Misuse any Granicus resources or cause any disruption, including but not limited to, the display of pornography or linking to pornographic material, advertisements, solicitations, or mass mailings to individuals who have not agreed to be contacted;

2.3.2. Use any process, program, or tool for gaining unauthorized access to the systems, networks, or accounts of other parties, including but not limited to, other Granicus Clients;

2.3.3. Client must not use the Granicus Products and Services in a manner in which system or network resources are unreasonably denied to other Granicus clients;

2.3.4. Client must not use the Services as a door or signpost to another server.

2.3.5. Access or use any portion of Granicus Products and Services, except as expressly allowed by this Agreement or each Order placed hereunder;

2.3.6. Disassemble, decompile, or otherwise reverse engineer all or any portion of the Granicus Products and Services;

2.3.7. Use the Granicus Products and Services for any unlawful purposes;

2.3.8. Export or allow access to the Granicus Products and Services in violation of U.S. laws or regulations;

2.3.9. Except as expressly permitted in this Agreement, subcontract, disclose, rent, or lease the Granicus Products and Services, or any portion thereof, for third party use; or

2.3.10. Modify, adapt, or use the Granicus Products and Services to develop any software application intended for resale which uses the Granicus Products and Services in whole or in part.

2.4. Client Feedback. Client assigns to Granicus any suggestion, enhancement, request, recommendation, correction or other feedback provided by Client relating to the use of the Granicus Products and Services. Granicus may use such submissions as it deems appropriate in its sole discretion.

2.5. Reservation of Rights. Subject to the limited rights expressly granted hereunder, Granicus and/or its licensors reserve all right, title and interest in the Granicus Products and Services, the documentation and resulting product including all related intellectual property rights. Further, no implied licenses are granted to Client. The Granicus name, the Granicus logo, and the product names associated with the services are trademarks of Granicus or its suppliers, and no right or license is granted to use them.

3. Representations, Warranties and Disclaimers

3.1. Representations. Each Party represents that it has validly entered into this Agreement and has the legal power to do so.

3.2. Warranties. Granicus warrants that it takes all precautions that are standard in the industry to increase the likelihood of a successful performance for the Granicus Products and Services; however, the Granicus Products and Services are provided "AS IS" and as available.

3.3. Disclaimers. EXCEPT AS PROVIDED IN SECTIONS 3.2 ABOVE, EACH PARTY HEREBY DISCLAIMS ANY AND ALL OTHER WARRANTIES OF ANY NATURE WHATSOEVER WHETHER

ORAL AND WRITTEN, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. GRANICUS DOES NOT WARRANT THAT GRANICUS PRODUCTS AND SERVICES WILL MEET CLIENT'S REQUIREMENTS OR THAT THE OPERATION THEREOF WILL BE UNINTERRUPTED OR ERROR FREE.

4. Confidential Information

4.1. Confidential Information. It is expected that one Party (Disclosing Party) may disclose to the other Party (Receiving Party) certain information which may be considered confidential and/or trade secret information ("Confidential Information"). Confidential Information shall include: (i) Granicus' Products and Services, (ii) non-public information if it is clearly and conspicuously marked as "confidential" or with a similar designation at the time of disclosure; (iii) non-public information of the Disclosing Party if it is identified as confidential and/or proprietary before, during, or promptly after presentation or communication and (iv) any information that should be reasonably understood to be confidential or proprietary to the Receiving Party, given the nature of the information and the context in which disclosed.

Each Receiving Party agrees to receive and hold any Confidential Information in strict confidence. Without limiting the scope of the foregoing, each Receiving Party also agrees: (a) to protect and safeguard the Confidential Information against unauthorized use, publication or disclosure; (b) not to reveal, report, publish, disclose, transfer, copy or otherwise use any Confidential Information except as specifically authorized by the Disclosing Party; (c) not to use any Confidential Information for any purpose other than as stated above; (d) to restrict access to Confidential Information to those of its advisors, officers, directors, employees, agents, consultants, contractors and lobbyists who have a need to know, who have been advised of the confidential nature thereof, and who are under express written obligations of confidentiality or under obligations of confidentiality imposed by law or rule; and (e) to exercise at least the same standard of care and security to protect the confidentiality of the Confidential Information received by it as it protects its own confidential information.
If a Receiving Party is requested or required in a judicial, administrative, or governmental proceeding to disclose any Confidential Information, it will notify the Disclosing Party as promptly as practicable so that the Disclosing Party may seek an appropriate protective order or waiver for that instance.

4.2. Exceptions. Confidential Information shall not include information which: (i) is or becomes public knowledge through no fault of the Receiving Party; (ii) was in the Receiving Party's possession before receipt from the Disclosing Party; (iii) is rightfully received by the Receiving party from a third party without any duty of confidentiality; (iv) is disclosed by the Disclosing Party without any duty of confidentiality on the third party; (v) is independently developed by the Receiving Party without use or reference to the Disclosing Party's Confidential Information; or (vi) is disclosed with the prior written approval of the Disclosing Party.

4.3. Storage and Sending. In the event that Granicus Products and Services will be used to store and/or send Confidential Information, Granicus must be notified in writing, in advance of the storage or sending. Should Client provide such notice, Client must ensure that Confidential Information or sensitive information is stored behind a secure interface and that Granicus Products and Services be used only to notify people of updates to the information that can be accessed after authentication against a secure interface managed by Client. Client is ultimately accountable for the security and privacy of data held by Granicus on its behalf.

4.4. Return of Confidential Information. Each Receiving Party shall return or destroy the Confidential Information immediately upon written request by the Disclosing Party; provided, however, that each Receiving Party may retain one copy of the Confidential Information in order to comply with applicable laws and the terms of this Agreement. Client understands and agrees that it may not always be possible to completely remove or delete all personal data from Granicus' databases without some residual data because of backups and for other reasons.

5. Term and Termination

5.1. Agreement Term. The Agreement Term shall begin on the Effective Date of the Agreement and continue for twelve (12) months. Unless a Party has given written notice to the other Party at least ninety (90) days prior to the end of the then-current annual term, the Granicus Products and Services will automatically renew at the end of each annual term for one (1) year.

5.2. Effect of Termination. If the Parties agree to terminate this Agreement and an Order is still in effect at the time of termination, then the terms and conditions contained in this Agreement shall continue to govern the outstanding Order until termination or expiration thereof. If the Agreement is terminated for breach, then unless otherwise agreed to in writing, all outstanding Orders shall immediately terminate as of the Agreement termination date.

5.3. Termination for Cause. The non-breaching Party may terminate this Agreement upon written notice if the other Party is in material breach of this Agreement and fails to cure such breach within thirty (30) days after the non-breaching Party provides written notice of the breach. A Party may also terminate this Agreement immediately upon notice if the other Party: (a) is liquidated, dissolved, or adjudged to be in a state of bankruptcy or receivership; (b) is insolvent, unable to pay its debts as they become due, makes an assignment for the benefit of creditors or takes advantage or any law for the benefit of debtors; or (c) ceases to conduct business for any reason on an ongoing basis leaving no successor in interest.

5.4. Survival. All rights granted hereunder shall terminate upon the latter of the termination or expiration date of this Agreement, or each Order. The provisions of this Agreement with respect to warranties, liability, choice of law and jurisdiction, and confidentiality shall survive termination of this Agreement and continue in full force and effect.

6. Limitation of Liability

6.1. EXCLUSION OF CONSEQUENTIAL AND RELATED DAMAGES. UNDER NO CIRCUMSTANCES SHALL GRANICUS BE LIABLE FOR ANY SPECIAL, INDIRECT, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, GRANICUS SHALL NOT BE LIABLE FOR: (A) ERROR OR INTERRUPTION OF USE OR FOR LOSS OR INACCURACY OR CORRUPTION OF CLIENT DATA; (B) COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY; (C) LOSS OF BUSINESS; (D) DAMAGES ARISING OUT OF ACCESS TO OR INABILITY TO ACCESS THE SERVICES, SOFTWARE, CONTENT, OR RELATED TECHNICAL SUPPORT; OR (E) FOR ANY MATTER BEYOND GRANICUS' REASONABLE CONTROL, EVEN IF GRANICUS HAS BEEN ADVISED OF THE POSSIBILITY OF ANY OF THE FOREGOING LOSSES OR DAMAGES.

6.2. LIMITATION OF LIABILITY. EXCEPT FOR CLIENT'S BREACH OF SECTION 2.3, IN NO INSTANCE SHALL EITHER PARTY'S LIABILITY TO THE OTHER PARTY FOR DIRECT DAMAGES UNDER THIS AGREEMENT (WHETHER IN CONTRACT OR TORT OR OTHERWISE) EXCEED THE FEES PAID BY CLIENT FOR THE GRANICUS PRODUCTS AND SERVICES DURING THE SIX (6) MONTHS IMMEDIATELY PRECEDING THE DATE THE DAMAGED PARTY NOTIFIES THE OTHER PARTY IN WRITING OF THE CLAIM FOR DIRECT DAMAGES. GRANICUS SHALL NOT BE RESPONSIBLE FOR

ANY LOST PROFITS OR OTHER DAMAGES, INCLUDING DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR ANY OTHER DAMAGES, HOWEVER CAUSED. NEITHER PARTY MAY INSTITUTE AN ACTION IN ANY FORM ARISING OUT OF NOR IN CONNECTION WITH THIS AGREEMENT MORE THAN TWO (2) YEARS AFTER THE CAUSE OF ACTION HAS ARISEN.

7. General

7.1. Relationship of the Parties. Granicus and Client acknowledge that they operate independent of each other. Nothing in this Agreement shall be deemed or construed to create a joint venture, partnership, agency, or employee/employer relationship between the Parties for any purpose, including, but not limited to, taxes or employee benefits. Each Party will be solely responsible for the payment of all taxes and insurance for its employees and business operations.

7.2. Headings. The various section headings of this Agreement are inserted only for convenience of reference and are not intended, nor shall they be construed to modify, define, limit, or expand the intent of the Parties.

7.3. Severability. To the extent permitted by applicable law, the Parties hereby waive any provision of law that would render any clause of this Agreement invalid or otherwise unenforceable in any respect. In the event that a provision of this Agreement is held to be invalid or otherwise unenforceable, such provision will be interpreted to fulfill its intended purpose to the maximum extent permitted by applicable law, and the remaining provisions of this Agreement will continue in full force and effect.

7.4. Assignment. Neither Party may assign, delegate, or otherwise transfer this Agreement or any of its rights or obligations hereunder, either voluntarily or by operation of law, without the prior written consent of the other Party (such consent not to be unreasonably withheld); provided, however, that either Party may assign this Agreement without the other Party's consent in the event of any successor or assign that has acquired all, or substantially all, of the assigning Party's business by means of merger, stock purchase, asset purchase, or otherwise. Any assignment or attempted assignment in violation of this Agreement shall be null and void.

7.5. Force Majeure. Any delay in the performance by either Party hereto of its obligations hereunder shall be excused when such delay in performance is due to any cause or event of any nature whatsoever beyond the reasonable control of such Party, including, without limitation, any act of God; any fire, flood, or weather condition; any computer virus, worm, denial of service attack; any earthquake; any act of a public enemy, war, insurrection, riot, explosion or strike; provided, that written notice thereof must be given by such Party to the other Party within twenty (20) days after occurrence of such cause or event.

7.6. Choice of Law and Jurisdiction. This Agreement shall be governed by and interpreted under the laws of the state in which the Client is located, without reference to the State's principles of conflicts of law. The Parties expressly consent and submit to the exclusive jurisdiction of the state and federal courts of the state in which the Client is located.

7.7. Entire Agreement. This Agreement, together with all Orders referenced herein, sets forth the entire understanding of the Parties with respect to the subject matter of this Agreement, and supersedes any and all prior oral and written understandings, quotations, communications, and agreements. Granicus and Client agree that any and all Orders are incorporated herein by this reference. In the event of possible conflict or inconsistency between such documents, the conflict or inconsistency shall be resolved by giving precedence in the following order: (1) the terms of this Agreement; (2) Orders; (3) all other SOWs or other purchase documents; (4) Granicus response to Client's request for RFI, RFP, RFQ; and (5) Client's RFI, RFP, RFQ. If Client issues a purchase order, Granicus hereby rejects any additional or conflicting terms appearing on the purchase order or any other ordering materials submitted by Client.

7.8. Reference. Notwithstanding any other terms to the contrary contained herein, Client grants Granicus the right to use Client's name and logo in Client lists and marketing materials.

7.9. Injunctive Relief. Granicus is entitled to obtain injunctive relief if Client's use of Granicus Products and Services is in violation of any restrictions set forth in this Agreement.

Granicus		Orange County CA	
By:	DocuSigned by: Bernadette Foley 06CBB3E1AA51459... (Authorized Signature)	**By:**	(Authorized Signature)
Name:	Bernadette Foley (Print or Type Name of Signatory)	**Name:**	(Print or Type Name of Signatory)
Title:	Sr. Manager, Renewals	**Title:**	
Date:	5/20/2026 (Execution Date)	**Date:**	(Execution Date)

GRANICUS

granicus.com | info@granicus.com

Regional Hours of Availability and Support Contact Channels

Region	Regular Support Hours	Support Contact Channels
USA	Monday - Friday, 8:00 AM - 5:00 PM Local time Excluding Federal Holidays	support.granicus.com 1-800-314-0147
Canada	Monday - Friday, 8:00 AM - 5:00 PM Local time Excluding Statutory Holidays	support.granicus.com 1-800-314-0147 Government of Canada direct line: +1 833-574-3559
Europe	Monday - Friday, 9:00 AM - 5:00 PM GMT Excluding Statutory Holidays	support.granicus.com +44 (0) 800 032 7764
Australia & New Zealand	Monday - Friday, 9:00 AM - 5:30 PM AEST Excluding National Holidays and Victorian Public Holidays	support.granicus.com +61 3 9913 0020
LAC	Monday - Friday, 9:00 AM - 5:00 PM GMT Excluding Statutory Holidays	support.granicus.com 1-800-314-0147 Spanish help desk: 1-800-TBD
Subscribers GovDelivery Help	Monday - Friday, 8:00 AM - 8:00 PM EST	subscriberhelp.granicus.com subscriberhelp@granicus.com 1-800-439-1420 USA +44 (0) 808 234 7450 Europe
24/7 Virtual Agent is available at support.granicus.com to answer transactional request and knowledge-oriented questions. Current System Status for Granicus Services and Applications. Update on platform Granicus System Status		

Extended Availability for Video Streaming Solution

Extended Hours for Live Meeting Support: The availability for the Live Meetings solution is extended to 11:30 PM local Time based on customer time zone (in the USA and Canada).

GRANICUS

granicus.com | info@granicus.com

Emergency Support

- Under Granicus Standard Support terms: Emergency technical support is available **24/7** by phone only for customers with live meetings solutions and Website when experiencing a **Level 1 outage** as defined below.

Technical Support Severity Level Definitions

Severity Level	Description	Time to 1st Response	Granicus Action
Level 1 (EMERGENCY)	Incident represents complete unavailability of the Granicus Products for all users, and no workaround is available	Within **two (2) hours**	Incident response process initiated immediately. Work on resolution starts immediately (24/7/365). Updates provided via case or status.granicus.com.
Level 2 (SEVERELY IMPAIRED)	Major feature failure with no workaround available	Within **four (4) hours**	Incident response process initiated. Work on resolution begins immediately. Updates provided via case or status.granicus.com.
Level 3 (IMPAIRED)	A primary feature is not working as expected but a workaround is available	Within **one (1) business day**	Case assigned and resolution work begins within 1 business day. After-hours cases are assigned on the next business day.
Level 4 (LOW IMPACT)	Incident has limited business impact; primary functionality is unaffected	Within **three (3) business days**	Case assigned and work on resolution begins within 3 business days. After-hours cases are assigned on the next business day.
Granicus shall use commercially reasonable efforts to resolve incidents affecting Granicus Products. Incidents that require debugging of programming code may need to be corrected during the next regular update cycle. Resolution time will be based on the details and severity of an incident. Regular follow-ups will be communicated with the customer until final resolution is reached.			

GRANICUS

granicus.com | info@granicus.com

GXC Service Levels for Enhanced and Advanced Technical Support

Service Levels	GXC Essentials & Operations Cloud	GXC Enhanced	GXC Advanced	Operations Cloud Video incident line
Level 1 (EMERGENCY)	1 hour	1 hour	30 minutes	15 minutes
Level 2 (SEVERELY IMPAIRED)	4 hours	2 hours	1 hour	
Level 3 (IMPAIRED)	12 hours (*)	5 hours (*)	2 hours (*)	
Level 4 (LOW IMPACT)	24 hours (*)	12 hours (*)	5 hours (*)	
24x7 sev1 Incident Line	5 minutes	5 minutes	5 minutes	15 minutes
(*) sev3 and sev4 target response time and service levels: responses and updates are shared during business hours only. Target response time carries into subsequent business days. Emails have no severity level and are answered within 24 hours.				

24/7 Technical Support Coverage

- **Level 1 coverage**: Available 24/7 for all GXC customers experiencing a Level 1 outage on any product part of GXC solution.
- **Level 1 & Level 2 coverage**: Available 24/7 for customers subscribed to GXC Enhanced and Advanced Editions.
- **Video Incident Line**: Available 24/7 for GXC Operations Cloud customers experiencing Level 1 outages.

Severity Level Updates Frequency

- **Level 1 & Level 2 Updates Frequency**:
  - **GXC Enhanced**: 24 hours, 48 hours
  - **GXC Advanced**: Twice per day, 24 hours

Product Availability

Granicus will use commercially reasonable efforts to make the Granicus Products Available 99.9% of the Available Hours of Operation, calculated on a calendar quarter basis, as follows:

[(Total time in a quarter – Unexpected Downtime – Scheduled Downtime – Service Disruption) / (Total time in a quarter – Schedule Downtime – Service Disruption)] * 100

Reasonable efforts are made to avoid Scheduled Downtime to perform maintenance; however, in circumstances where Scheduled Downtime is required, notification will be posted at least 10 days in advance for all Product Suites. Scope of maintenance activities may be refined to ensure adherence to published schedule. Customers can subscribe to product specific email notifications on the status page status.granicus.com

Notifications for Granicus Products of any system-wide outages will be posted to status.granicus.com and will occur within one (1) hour from the time the issues are first recognized by Granicus.

Reports of Unscheduled Downtime will be provided upon request up to once per calendar quarter.

Term	Definition
Availability	Ability of a user to access the Granicus Product via the Internet. Granicus uses industry-standard third-party monitoring to measure Availability through URL monitoring (HTTP).
Available Hours of Operation	Twenty-four hours a day, seven days per week, minus Scheduled Downtime.
Maintenance	Updates, upgrades, bug fixes, and patches to the Granicus Products. Maintenance times vary by Product. An up-to-date maintenance schedule can be found at status.granicus.com.
Scheduled Downtime	Is the period when the Granicus Product may be inaccessible to permit Granicus to perform Maintenance services.
Service Disruption	Is the downtime arising from causes beyond the reasonable direct control of Granicus, such as the interruption or failure of digital transmission links or telecommunications, hostile network attacks, or issues arising with customer Domain Name Systems (DNS).
Unexpected Downtime	Is any time after the first five minutes of downtime where the Granicus Product is not Available in any way.

Outage credit

Any credit provided within this Technical Support and Availability document will be referred to as an **Outage Credit**. The Outage Credit shall be applied as credit to the customer's following renewal term for the customer's affected Granicus Product and will be added to the end of the then-current period of performance and shall be provided upon the customer's request.

Outage Credit is available solely to the extent Unscheduled Downtime created unavailability of the entire Granicus product. In no event shall any credit for a calendar quarter exceed the seven (7) days of Outage Credit. Granicus shall have the ability to determine at its reasonable discretion whether Unscheduled Downtime has occurred.

Per calendar quarter, Granicus will provide Outage Credit as follows:

Site Outage per Quarter (Unless Otherwise Specified Below)	**Amount of Outage Credit** (Unless Otherwise Specified Below)
>99.9%	No Outage Credit
99.8-98.0%	1 day credit
97.9-97.0%	3 days credit
96.9% or less	7 days credit