# ATTACHMENT C.1

# COUNTY - INFORMATION SECURITY AND PRIVACY REQUIREMENTS

# FOR

# DEFENSE AND LAW ENFORCEMENT SOLUTION

# ATTACHMENT C.1
# COUNTY - INFORMATION SECURITY AND PRIVACY REQUIREMENTS

The County of Los Angeles (County) is committed to safeguarding the Integrity (as defined below) of the County systems, Data, Information and protecting the privacy rights of the individuals that it serves. This Information Security and Privacy Requirements Attachment (Attachment) sets forth the County and the Contractor's commitment and agreement to fulfill each of their respective obligations under applicable local, state or federal laws, rules, or regulations, as well as applicable industry standards concerning privacy, Data protections, Information Security, Confidentiality, Availability, and Integrity of such Information. The Information Security and privacy requirements and procedures in this Attachment are to be established by Contractor before the effective date of the Contract and maintained throughout the Term of the Contract.

These requirements and procedures are minimum standards and are in addition to the requirements of the underlying base agreement between the County and Contractor and any other agreements between the parties. However, it is Contractor's sole obligation to: (i) implement appropriate and reasonable measures to secure and protect its systems and all County Information against internal and external Threats and Risks; and (ii) continuously review and revise those measures to address ongoing Threats and Risks. Failure to comply with the minimum requirements and procedures set forth in this Attachment will constitute a material, non-curable breach of Contract by Contractor, entitling the County, in addition to the cumulative of all other remedies available to it at law, in equity, or under the Contract, to immediately terminate the Contract. To the extent there are conflicts between this Attachment and the Contract, this Attachment will prevail unless stated otherwise.

## 1. DEFINITIONS

Unless otherwise defined in the Contract, the definitions herein contained are specific to the uses within this Exhibit.

a. **Availability:** the condition of Information being accessible and usable upon demand by an authorized entity (Workforce Member or process).

b. **Confidentiality:** the condition that Information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the Information.

c. **County Information:** all Data and Information belonging to the County.

d. **Data:** a subset of Information comprised of qualitative or quantitative values.

e. **Incident:** a suspected, attempted, successful, or imminent Threat of unauthorized electronic and/or physical access, use, disclosure, breach, modification, or destruction of information; interference with Information Technology operations; or significant violation of County policy.

f. **Information:** any communication or representation of knowledge or understanding such as facts, Data, or opinions in any medium or form, including electronic, textual,

numerical, graphic, cartographic, narrative, or audiovisual.

g. **Information Security Policy:** high level statements of intention and direction of an organization used to create an organization's Information Security Program as formally expressed by its top management.

h. **Information Security Program:** formalized and implemented Information Security Policies, standards and procedures that are documented describing the program management safeguards and common controls in place or those planned for meeting the County's information security requirements.

i. **Information Technology:** any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of Data or Information.

j. **Integrity**: the condition whereby Data or Information has not been improperly modified or destroyed and authenticity of the Data or Information can be ensured.

k. **Mobile Device Management (MDM):** software that allows Information Technology administrators to control, secure, and enforce policies on smartphones, tablets, and other endpoints.

l. **Privacy Policy:** high level statements of intention and direction of an organization used to create an organization's Privacy Program as formally expressed by its top management.

m. **Privacy Program:** a formal document that provides an overview of an organization's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the organization's privacy official and other staff, the strategic goals and objectives of the Privacy Program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

n. **Risk:** a measure of the extent to which the County is threatened by a potential circumstance or event, Risk is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

o. **Threat:** any circumstance or event with the potential to adversely impact County operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an Information System via unauthorized access, destruction, disclosure, modification of Information, and/or denial of service.

p. **Vulnerability:** a weakness in a system, application, network or process that is subject to exploitation or misuse.

q. **Workforce Member:** employees, volunteers, and other persons whose conduct, in the performance of work for Los Angeles County, is under the direct control of Los Angeles County, whether or not they are paid by Los Angeles County. This includes, but may not be limited to, full and part time elected or appointed officials, employees,

affiliates, associates, students, volunteers, and staff from third party entities who provide service to the County.

## 2. INFORMATION SECURITY AND PRIVACY PROGRAMS

a. **Information Security Program.** Contractor must maintain a company-wide Information Security Program designed to evaluate Risks to the Confidentiality, Availability, and Integrity of the County Information covered under this Contract.

Contractor's Information Security Program must include the creation and maintenance of Information Security Policies, standards, and procedures. Information Security Policies, standards, and procedures will be communicated to all Contractor employees in a relevant, accessible, and understandable form and will be regularly reviewed and evaluated to ensure operational effectiveness, compliance with all applicable laws and regulations, and addresses new and emerging Threats and Risks.

Contractor must exercise the same degree of care in safeguarding and protecting County Information that Contractor exercises with respect to its own Information and Data, but in no event less than a reasonable degree of care. Contractor must implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the Confidentiality, Integrity, and Availability of County Information.

Contractor's Information Security Program must:

- Protect the Confidentiality, Integrity, and Availability of County Information in the Contractor's possession or control,
- Protect against any anticipated Threats or hazards to the Confidentiality, Integrity, and Availability of County Information,
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of County Information,
- Protect against accidental loss or destruction of, or damage to, County Information, and
- Safeguard County Information in compliance with any applicable laws and regulations which apply to Contractor.

b. **Privacy Program.** Contractor must establish and maintain a company-wide Privacy Program designed to incorporate Privacy Policies and practices in its business operations to provide safeguards for Information, including County Information. Contractor's Privacy Program must include the development of, and ongoing reviews and updates to Privacy Policies, guidelines, procedures and appropriate workforce privacy training within its organization. These Privacy Policies, guidelines, procedures, and appropriate training will be provided to all Contractor employees, agents, and volunteers. Contractor's Privacy Policies, guidelines, and procedures must be continuously reviewed and updated for effectiveness and compliance with applicable

laws and regulations, and to appropriately respond to new and emerging Threats and Risks. Contractor's Privacy Program must perform ongoing monitoring and audits of operations to identify and mitigate privacy Threats.

Contractor must exercise the same degree of care in safeguarding the privacy of County Information that Contractor exercises with respect to its own Information, but in no event less than a reasonable degree of care. Contractor will implement, maintain, and use appropriate privacy practices and protocols to preserve the Confidentiality of County Information.

Contractor's Privacy Program must include:

- A Privacy Program framework that identifies and ensures that Contractor complies with all applicable laws and regulations,
- External privacy policies, and internal privacy policies, procedures and controls to support the privacy program,
- Protections against unauthorized or unlawful access, use, disclosure, alteration, or destruction of County Information,
- A training program that covers Privacy Policies, protocols and awareness,
- A response plan to address privacy Incidents and privacy breaches, and
- Ongoing privacy assessments and audits.

## 3. PROPERTY RIGHTS TO COUNTY INFORMATION

All County Information is deemed property of the County, and the County will retain exclusive rights and ownership thereto. County Information must not be used by Contractor for any purpose other than as required under this Contract, nor will such or any part of such be disclosed, sold, assigned, leased, or otherwise disposed of, to third parties by Contractor, or commercially exploited or otherwise used by, or on behalf of, Contractor, its officers, directors, employees, or agents. Contractor may assert no lien on or right to withhold from the County, any County Information it receives from, receives addressed to, or stores on behalf of, the County. Notwithstanding the foregoing, Contractor may aggregate, compile, and use County Information in order to improve, develop or enhance the System Software and/or other services offered, or to be offered, by Contractor, provided that (i) no County Information in such aggregated or compiled pool is identifiable as originating from, or can be traced back to the County, and (ii) such Data or Information cannot be associated or matched with the identity of an individual alone, or linkable to a specific individual. Contractor specifically consents to the County's access to such County Information held, stored, or maintained on any and all devices Contactor owns, leases or possesses.

## 4. CONTRACTOR'S USE OF COUNTY INFORMATION

Contractor may use County Information only as necessary to carry out its obligations under this Contract. Contractor must collect, maintain, or use County Information only for the purposes specified in the Contract and, in all cases, in compliance with all applicable local, state, and federal laws and regulations governing the collection, maintenance, transmission, dissemination, storage, use, and destruction of County Information, including, but not limited to: (i) any local, state and federal law governing the protection of personal Information, (ii) any local, state and federal security breach notification laws, and (iii) the rules, regulations and directives of the Federal Trade Commission, as amended from time to time.

## 5. SHARING COUNTY INFORMATION AND DATA

Contractor must not share, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, County Information to a third party for monetary or other valuable consideration.

## 6. CONFIDENTIALITY

a. **Confidentiality of County Information**. Contractor agrees that all County information is Confidential and proprietary to the County regardless of whether such information was disclosed intentionally or unintentionally, or marked as "confidential."

b. **Disclosure of County Information.** Contractor may disclose County Information only as necessary to carry out its obligations under this Contract, or as required by law, and is prohibited from using County Information for any other purpose without the prior express written approval of the County's contract administrator in consultation with the County's Chief Information Security Officer and/or Chief Privacy Officer. If required by a court of competent jurisdiction or an administrative body to disclose County Information, Contractor must notify the County's contract administrator immediately and prior to any such disclosure, to provide the County an opportunity to oppose or otherwise respond to such disclosure, unless prohibited by law from doing so.

c. **Disclosure Restrictions of Non-Public Information.** While performing work under this Contract, Contractor may encounter County Non-public Information ("NPI") in the course of performing this Contract, including, but not limited to, licensed technology, drawings, schematics, manuals, sealed court records, and other materials described and/or identified as "Internal Use", "Confidential" or "Restricted" as defined in Board of Supervisors Policy 6.104 – Information Classification Policy as NPI. Contractor must not disclose or publish any County NPI and material received or used in performance of this Contract. This obligation is perpetual.

d. **Individual Requests.** Contractor must acknowledge any request or instructions from the County regarding the exercise of any individual's privacy rights provided under applicable federal or state laws. Contractor must have in place appropriate policies and procedures to promptly respond to such requests and comply with any request or instructions from the County within seven Days. If an individual makes a request directly to Contractor involving County Information, Contractor must notify the County within five Days and the County will coordinate an appropriate response, which may include instructing Contractor to assist in fulfilling the request. Similarly, if Contractor receives a privacy or security complaint from an individual regarding County Information, Contractor must notify the County as described in Section 13 SECURITY AND PRIVACY INCIDENTS, and the County will coordinate an appropriate response.

e. **Retention of County Information.** Contractor must not retain any County Information for any period longer than necessary for Contractor to fulfill its obligations under the Contract and applicable law, whichever is longest.

## 7. SUBCONTRACTORS AND THIRD PARTIES

The County acknowledges that in the course of performing its services, Contractor may desire or require the use of goods, services, and/or assistance of Subcontractors or other third parties or suppliers. The terms of this Attachment must also apply to all Subcontractors and third parties. Contractor or third party must be subject to the following terms and conditions: (i) each third party must agree in writing to comply with and be bound by the applicable terms and conditions of this Attachment, both for itself and to enable Contractor to be and remain in compliance with its obligations hereunder, including those provisions relating to Confidentiality, Integrity, Availability, disclosures, security, and such other terms and conditions as may be reasonably necessary to effectuate the Contract including this Attachment; and (ii) Contractor must be and remain fully liable for the acts and omissions of each Subcontractor and third party, and fully responsible for the due and proper performance of all Contractor obligations under this Contract.

Contractor must obtain advanced approval from the County's Chief Information Security Officer and/or Chief Privacy Officer prior to subcontracting services subject to this Attachment.

## 8. STORAGE AND TRANSMISSION OF COUNTY INFORMATION

All County Information must be rendered unusable, unreadable, or indecipherable to unauthorized individuals. Without limiting the generality of the foregoing, Contractor will encrypt all workstations, portable devices (such as mobiles, wearables, and tablets) and removable media (such as portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) that store County Information in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise approved by the County's Chief Information Security Officer.

Contractor will encrypt County Information transmitted on networks outside of Contractor's control with Transport Layer Security (TLS) or Internet Protocol Security **(**IPSec**)**, at a minimum cipher strength of 128 bit or an equivalent secure transmission protocol or method approved by County's Chief Information Security Officer.

In addition, any cloud storage of County Information must reside in CJIS compliant cloud providers only. All mobile devices storing County Information must be managed by a Mobile Device Management system. Such system must provide provisions to enforce a password/passcode on enrolled mobile devices. All workstations/Personal Computers (including laptops, 2-in-1s, and tablets) will maintain the latest operating system security patches, and the latest virus definitions. Virus scans must be performed at least monthly. Request for less frequent scanning must be approved in writing by the County's Chief Information Security Officer.

## 9. RETURN OR DESTRUCTION OF COUNTY INFORMATION

Contractor must return or destroy County Information in the manner prescribed in this section unless the Contract prescribes procedures for returning or destroying County Information and those procedures are no less stringent than the procedures described in this section.

a. **Return or Destruction.** Upon County's written request, or upon expiration or termination of this Contract for any reason, Contractor must: (i) promptly return or destroy, at the County's option, all originals and copies of all documents and materials it has received containing County Information; or (ii) if return or destruction is not permissible under applicable law, continue to protect such Information in accordance with the terms of this Contract; and (iii) deliver or destroy, at the County's option, all originals and copies of all summaries, records, descriptions, modifications, negatives, drawings, adoptions and other documents or materials, whether in writing or in machine-readable form, prepared by Contractor, prepared under its direction, or at its request, from the documents and materials referred to in Subsection (i) of this Section. For all documents or materials referred to in Subsections (i) and (ii) of this Section that the County requests be returned to the County, Contractor must provide a written attestation on company letterhead certifying that all documents and materials have been delivered to the County. For documents or materials referred to in Subsections (i) and (ii) of this Section that the County requests be destroyed, Contractor must provide an attestation on company letterhead and certified documentation from a media destruction firm consistent with subdivision b below of this Section. Upon termination or expiration of the Contract or at any time upon the County's request, Contractor must return all hardware, if any, provided by the County to Contractor. The hardware should be physically sealed and returned via a bonded courier, or as otherwise directed by the County.

b. **Method of Destruction.** Contractor must destroy all originals and copies by (i) cross-cut shredding paper, film, or other hard copy media so that the Information cannot be read or otherwise reconstructed; and (ii) purging or destroying electronic media

containing County Information consistent with NIST Special Publication 800-88, "Guidelines for Media Sanitization" such that the County Information cannot be retrieved. Contractor will provide an attestation on company letterhead and certified documentation from a media destruction firm, detailing the destruction method used and the County Information involved, the date of destruction, and the company or individual who performed the destruction. Such statement will be sent to the designated County contract manager within ten Days of termination or expiration of the Contract or at any time upon the County's request. On termination or expiration of this Contract, the County will return or destroy all Contractor's Information marked as confidential (excluding items licensed to the County hereunder, or that provided to the County by the Contractor hereunder), at the County's option.

## 10. PHYSICAL AND ENVIRONMENTAL SECURITY

All Contractor facilities that process County Information will be located in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physically secure environment from unauthorized access, damage, and interference.

All Contractor facilities that process County Information will be maintained with physical and environmental controls (temperature and humidity) that meet or exceed hardware manufacturer's specifications.

## 11. OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY

Contractor must: (i) monitor and manage all of its Information processing facilities, including, without limitation, implementing operational procedures, change management, and Incident response procedures consistent with Section 13 SECURITY AND PRIVACY INCIDENTS; and (ii) deploy adequate anti-malware software and adequate back-up systems to ensure essential business Information can be promptly recovered in the event of a disaster or media failure; and (iii) ensure its operating procedures are adequately documented and designed to protect Information and computer media from theft and unauthorized access.

Contractor must have business continuity and disaster recovery plans. These plans must include a geographically separate back-up data center and a formal framework by which an unplanned event will be managed to minimize the loss of County Information and services. The formal framework includes a defined back-up policy and associated procedures, including documented policies and procedures designed to: (i) perform back-up of data to a remote back-up data center in a scheduled and timely manner; (ii) provide effective controls to safeguard backed-up data; (iii) securely transfer County Information to and from back- up location; (iv) fully restore applications and operating systems; and (v) demonstrate periodic testing of restoration from back-up location. If Contractor makes backups to removable media (as described in Section 8 STORAGE AND TRANSMISSION OF COUNTY INFORMATION), all such backups must be encrypted in

compliance with the encryption requirements noted above in Section 8 STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

## 12. ACCESS CONTROL

Subject to and without limiting the requirements under Section 8 STORAGE AND TRANSMISSION OF COUNTY INFORMATION, County Information (i) may only be made available and accessible to those parties explicitly authorized under the Contract or otherwise expressly approved by the County Project Director or Project Manager in writing; and (ii) if transferred using removable media (as described in Section 8 STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be sent via a bonded courier and protected using encryption technology designated by Contractor and approved by the County's Chief Information Security Officer in writing. The foregoing requirements must apply to back-up media stored by Contractor at off-site facilities.

Contractor must implement formal procedures to control access to County systems, services, and/or Information, including, but not limited to, user account management procedures and the following controls:

a. Network access to both internal and external networked services must be controlled, including, but not limited to, the use of industry standard and properly configured firewalls,

b. Operating systems will be used to enforce access controls to computer resources including, but not limited to, multi-factor authentication, use of virtual private networks (VPN), authorization, and event logging,

c. Contractor will conduct regular, no less often than semi-annually, user access reviews to ensure that unnecessary and/or unused access to County Information is removed in a timely manner,

d. Applications will include access control to limit user access to County Information and application system functions,

e. All systems will be monitored to detect deviation from access control policies and identify suspicious activity. Contractor must record, review and act upon all events in accordance with Incident response policies set forth in Section 13 SECURITY AND PRIVACY INCIDENTS, and

f. In the event any hardware, storage media, or removable media (as described in Section 8 STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be disposed of or sent off-site for servicing, Contractor must ensure all County Information, has been eradicated from such hardware and/or media using industry best practices as discussed in Section 8 STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

## 13. SECURITY AND PRIVACY INCIDENTS

In the event of a Security or Privacy Incident, Contractor must:

a. Promptly notify the County's Chief Information Security Officer, the Departmental Information Security Officer, and the County's Chief Privacy Officer of any Incidents involving County Information, within twenty-four (24) hours of detection of the Incident. All notifications must be submitted via encrypted email and telephone.

   **County Chief Information Security Officer and Chief Privacy Officer email**
   CISO-CPO_Notify@lacounty.gov

   **Chief Information Security Officer:**
   James Thurmond, (Acting) Chief Information Security Officer
   320 W Temple, 7th Floor
   Los Angeles, CA 90012
   (213) 253-5659

   **Chief Privacy Officer:**
   Lillian Russell, Chief Privacy Officer
   320 W Temple, 7th Floor
   Los Angeles, CA 90012
   (213) 351-5363

   **Departmental Information Security Officer:**
   Fransiscus X. Gunawan (Hendra), Departmental Information Security Officer
   12440 Imperial Hwy Suite 400 E
   Norwalk, CA 90650
   (562) 345-4181

b. Include the following Information in all notices:

   i. The date and time of discovery of the Incident,

   ii. The approximate date and time of the Incident,

   iii. A description of the type of County Information involved in the reported Incident,

   iv. A summary of the relevant facts, including a description of measures being taken to respond to and remediate the Incident, and any planned corrective actions as they are identified, and

   v. The name and contact information for the organizations official representative(s), with relevant business and technical information relating to the incident.

c. Cooperate with the County to investigate the Incident and seek to identify the specific County Information involved in the Incident upon the County's written request, without charge, unless the Incident has been confirmed to have been caused by the acts or omissions of the County. As Information about the Incident is collected or otherwise becomes available to Contractor, and unless prohibited by law, Contractor must provide Information regarding the nature and consequences of the Incident that are

reasonably requested by the County to allow the County to notify affected individuals, government agencies, and/or credit bureaus.

d. Immediately initiate the appropriate portions of their Business Continuity and/or Disaster Recovery plans in the event of an Incident causing an interference with Information Technology operations.

e. Assist and cooperate with forensic investigators, the County, law firms, and/or law enforcement agencies at the direction of the County to help determine the nature, extent, and source of any Incident, and reasonably assist and cooperate with the County on any additional disclosures that the County is required to make as a result of the Incident.

f. Allow the County or its third-party designee at the County's election to perform audits and tests of the Contractor's environment that may include, but are not limited to, interviews of relevant employees, review of documentation, or technical inspection of systems, as they relate to the receipt, maintenance, use, retention, and authorized destruction of County Information.

Notwithstanding any other provisions in the Contract and this Attachment, Contractor will be (i) liable for all damages and fines, (ii) responsible for all corrective action, and (iii) responsible for all notifications arising from an Incident involving County Information caused by Contractor's weaknesses, negligence, errors, or lack of Information Security or privacy controls or provisions.

## 14. NON-EXCLUSIVE EQUITABLE REMEDY

Contractor acknowledges and agrees that due to the unique nature of County Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach may result in irreparable harm to the County, and therefore, that upon any such breach, the County will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to additional remedies available within law or equity. Any breach of Confidentiality as outlined in Paragraph 17.0 (Confidentiality) and Attachment C.3 (Departmental Information Security Requirements) of the Contract, constitutes a material breach of this Contract and will be grounds for immediate termination of this Contract at the exclusive discretion of the County.

## 15. AUDIT AND INSPECTION

**a. Self-Audits.** Contractor must periodically conduct audits, assessments, testing of the system of controls, and testing of Information Security and privacy procedures, including penetration testing, intrusion detection, and firewall configuration reviews. These periodic audits will be conducted by staff certified to perform the specific audit in question at Contractor's sole cost and expense through either (i) an internal independent audit function, (ii) a nationally recognized, external, independent auditor, or (iii) another independent auditor approved by the County.

Contractor must have a process for correcting control deficiencies that have been identified in the periodic audit, including follow up documentation providing evidence of such corrections. Contractor must provide the audit results and any corrective action documentation to the County promptly upon its completion at the County's request. With respect to any other report, certification, or audit or test results prepared or received by Contractor that contains any County Information, Contractor must promptly provide the County with copies of the same upon the County's reasonable request, including identification of any failure or exception in the Contractor's Information systems, products, and services, and the corresponding steps taken by Contractor to mitigate such failure or exception. Any reports and related materials provided to the County pursuant to this Section must be provided at no additional charge to the County.

**b. County Requested Audits.** At its own expense, the County, or an independent third-party auditor commissioned by the County, will have the right to audit Contractor's infrastructure, security and privacy practices, Data center, services and/or systems storing or processing County Information via an onsite inspection at least once a year. Upon the County's request, Contractor must complete a questionnaire regarding Contractor's Information Security and/or program. The County will pay for the County requested audit unless the auditor finds that Contractor has materially breached this Attachment, in which case Contractor will bear all costs of the audit; and if the audit reveals material non-compliance with this Attachment, the County may exercise its termination rights underneath the Contract.

Such audit will be conducted during Contractor's normal business hours with reasonable advance notice, in a manner that does not materially disrupt or otherwise unreasonably and adversely affect Contractor's normal business operations. The County's request for the audit will specify the scope and areas (e.g., Administrative, Physical, and Technical) that are subject to the audit and may include, but are not limited to physical controls inspection, process reviews, policy reviews, evidence of external and internal Vulnerability scans, penetration test results, evidence of code reviews, and evidence of system configuration and audit log reviews. It is understood that the results may be filtered to remove the specific Information of other Contractor customers such as IP address, server names, etc. Contractor must cooperate with the County in the development of the scope and methodology for the audit, and the timing and implementation of the audit. This right of access will extend to any regulators with oversight of the County. Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes. When not prohibited by regulation, Contractor will provide to the County a summary of: (i) the results of any security audits, security reviews, or other relevant audits, conducted by Contractor or a third party; and (ii) corrective actions or modifications, if any, Contractor will implement in response to such audits.

## 16. CYBER LIABILITY INSURANCE

Refer to Paragraph 15.4 (Cyber Liability Insurance) of the Contract.

## 17. PRIVACY AND SECURITY INDEMNIFICATION

In addition to the indemnification provisions in the Contract, Contractor agrees to indemnify, defend, and hold harmless the County, its Special Districts, elected and appointed officers, agents, employees, and volunteers from and against any and all claims, demands liabilities, damages, judgments, awards, losses, costs, expenses or fees including reasonable attorneys' fees, accounting and other expert, consulting or professional fees, and amounts paid in any settlement arising from, connected with, or relating to:

- Contractor's violation of any federal and state laws in connection with its accessing, collecting, processing, storing, disclosing, or otherwise using County Information,
- Contractor's failure to perform or comply with any terms and conditions of this Contract or related agreements with the County, and/or
- Any Information loss, breach of Confidentiality, or Incident involving any County Information that occurs on Contractor's systems or networks (including all costs and expenses incurred by the County to remedy the effects of such loss, breach of Confidentiality, or Incident, which may include (i) providing appropriate notice to individuals and governmental authorities, (ii) responding to individuals' and governmental authorities' inquiries, (iii) providing credit monitoring to individuals, and (iv) conducting litigation and settlements with individuals and governmental authorities).

Notwithstanding the preceding sentences, the County will have the right to participate in any such defense at its sole cost and expense, except that in the event Contractor fails to provide the County with a full and adequate defense, as determined by the County in its sole judgment, the County will be entitled to retain its own counsel, including, without limitation, County Counsel, and to reimbursement from Contractor for all such costs and expenses incurred by the County in doing so. Contractor will not have the right to enter into any settlement, agree to any injunction or other equitable relief, or make any admission, in each case, on behalf of the County without the County's prior written approval.

## ADDENDUM C: APPLICATION SOURCE CODE REPOSITORY

Contractor must manage the source code in the manner prescribed in this Addendum unless the Contract prescribes procedures for managing the source code and those procedures are no less stringent than the procedures described in this addendum.

a. **County Application Source Code**. To facilitate the centralized management, reporting, collaboration, and continuity of access to the most current production version of application source code, all code, artifacts, and deliverables produced under this Contract, (hereinafter referred to as "County Source Code") must be version controlled, stored, and delivered on a single industry-standard private Git repository, provided, managed, and supported by the County. Upon commencement of the contract period, Contractor will be granted access to the County's private Git repository.

b. **Git Repository.** Contractor will use the County Git repository during the entire lifecycle of the project from inception to final delivery. Contractor will create and design documents, Data flow diagrams, security diagrams, configuration settings, software or hardware requirements and specifications, attribution to third-party code, libraries and all dependencies, and any other documentation related to all County Source Code and corresponding version-controlled documentation within the Git repository. This documentation must include an Installation Guide and a User Guide for the final delivered source code such that the County may download, install, and make full functional use of the delivered code as specified and intended.

# ATTACHMENT C.2

# SOLUTION RESPONSE-TIME REQUIREMENTS

# FOR

# DEFENSE AND LAW ENFORCEMENT SOLUTION

# ATTACHMENT C.2

## SOLUTION RESPONSE-TIME REQUIREMENTS (SYSTEMWIDE)

| Defense and Law Enforcement Solution – All Users | | |
|---|---|---|
| **Item No.** | **TRANSACTION DESCRIPTION** | **MAXIMUM RESPONSE-TIMES UNDER PEAK LOAD[1]** |
| **1** | Website load time | Three seconds maximum |
| **2** | Application load time | 10 seconds maximum |
| **3** | Login (ADFS) | Five seconds maximum |
| **4** | Post-login page load time | Three seconds maximum |
| **5** | Intra-application page transitions | Five seconds maximum |
| **6** | Generate preview for printing | Five seconds |
| **7 (a)** | Generate report PDF (1-10 pages) | 10 seconds |
| **7 (b)** | Additional increments of 10 pages | Two seconds |

| Defense and Law Enforcement Solution – End Users | | |
|---|---|---|
| **Item No.** | **TRANSACTION DESCRIPTION** | **MAXIMUM RESPONSE-TIMES UNDER PEAK LOAD[1]** |
| **8** | Ingest incoming image/record (i.e., photo images, photo scans) and display (20MB file size) | Five seconds |
| **9** | Response time per class of transaction (from receipt of transaction to response, | |
| **9 (a)** | • TP – TP | 30 seconds[2] |
| **9 (b)** | • TP – LT | 60 seconds[3] |
| **9 (c)** | • LT – TP | Three minutes[3] |
| **9 (d)** | • Palm LT – KP | Five minutes[3] |
| **9 (e)** | • KP - Palm LT | Three minutes[3] |
| **9 (f)** | • RAPID ID – ID4 TP-TP | 15 seconds[2] |
| **9 (g)** | • RAPID ID - IRIS ID TP-TP (IIDS) | 15 seconds[2] |
| **9 (h)** | • RAPID ID - Mobile ID TP – TP (TFS) | 15 seconds[2] |
| **9 (i)** | • RAPID ID - Mobile ID TP – TP (Contactless) | 15 seconds[2] |
| **10 (a)** | Thick client single field search (i.e., MAIN, SID, FBI) results | Two seconds |

# ATTACHMENT C.2

## SOLUTION RESPONSE-TIME REQUIREMENTS (SYSTEMWIDE)

| | | |
|---|---|---|
| **10 (b)** | Web single field search (i.e., MAIN, SID, FBI) results | Three seconds maximum |
| **11 (a)** | Thick client multi-field search (i.e., MAIN + SID + FBI, MAIN + FBI) results | Four seconds |
| **11 (b)** | Web multi-field search (i.e., MAIN + SID + FBI, MAIN + FBI) results | Five seconds maximum |
| **12** | Time between cycling through images | One second |
| **13** | Open a record to edit | Four seconds |
| **14** | Save record entries | Two seconds |
| **15** | Field validation for accuracy | 250 milliseconds |

| Solution Interface and System Administration | | |
|---|---|---|
| **Item No.** | **TRANSACTION DESCRIPTION** | **MAXIMUM RESPONSE-TIMES UNDER PEAK LOAD[1]** |
| **16** | Newly ingested NIST file (lights-out) available in Archive | Three minutes |
| **17** | Save an ABIS User's security rights | One second |
| **18** | Propagate changes to system parameters systemwide | Five seconds |
| **19** | Dashboard initial load time | Five seconds |
| **20** | Dashboard refresh load time | One second |
| **21** | Monitoring tool initial load time | Five seconds |
| **22** | Monitoring tool refresh load time | One second |

1. **Exclusive of County Network, speed measured from primary data center to LACRIS Offices in Norwalk**
2. **From time transaction is received to final results sent**
3. **From search launch time to results displayed back to user**

# ATTACHMENT C.3

# DEPARTMENTAL INFORMATION SECURITY REQUIREMENTS

# FOR

# DEFENSE AND LAW ENFORCEMENT SOLUTION

# DEPARTMENTAL INFORMATION SECURITY REQUIREMENTS

This Attachment C.3 sets forth information security procedures to be established by Contractor before the effective date of the Contract and maintained throughout the term of the Contract. These procedures are in addition to the requirements of the Contract and those required pursuant to Attachment C.2. They present a minimum standard only. However, it is Contractor's sole obligation to: (i) implement appropriate measures to secure its systems and data, including Personal Information, Protected Health Information and County's Confidential Information, against internal and external Threats and Risks; and (ii) continuously review and revise those measures to address ongoing Threats and Risks. Failure to comply with the minimum standards set forth in this Attachment will constitute a material, non-curable breach of the Contract by Contractor, entitling the County, in addition to and cumulative of all other remedies available to it at law, in equity, or under the Contract, to immediately terminate the Contract. Unless specifically defined in this Attachment, capitalized terms have the meanings set forth in the Contract.

## 1. SECURITY POLICY

Contractor must establish and maintain a formal, documented, mandated, company-wide information security program, including security policies, standards and procedures (**Information Security Policy**). The Information Security Policy will be communicated to all Contractor personnel in a relevant, accessible, and understandable form and will be regularly reviewed and evaluated to ensure its operational effectiveness, compliance with all applicable laws and regulations, and to address new threats and risks.

## 2. PERSONNEL AND CONTRACTOR PROTECTIONS

Contractor must screen and conduct background checks on all Contractor personnel who will have access to County's Confidential Information, including Personally Identifiable Information and Protected Health Information, for potential security risks and require all employees and contractors to sign an appropriate written confidentiality/non-disclosure agreement. All agreements with third parties involving access to Contractor's systems and data, including all outsourcing arrangements and maintenance and support agreements (including facilities maintenance), will specifically address security risks, controls, and procedures for information systems. Contractor must supply each of its Contractor personnel with appropriate, ongoing training regarding information security procedures, Risks, and Threats. Contractor must have an established set of procedures to ensure Contractor personnel promptly report actual and/or suspected breaches of security.

## 3. REMOVABLE MEDIA

Except in the context of Contractor's routine back-ups or as otherwise specifically authorized by County in writing, Contractor must institute strict security controls, including encryption of Removable Media (as defined below), to prevent transfer of Personally Identifiable Information and Protected Health Information to any form of Removable Media. For purposes of this Attachment, "**Removable Media**" means portable or removable hard disks, floppy disks, USB memory drives, zip disks, optical disks, CDs, DVDs, digital film, digital cameras, memory cards (e.g., Secure Digital (SD), Memory Sticks (MS), CompactFlash (CF), SmartMedia (SM), MultiMediaCard (MMC), and xD-Picture Card (xD)), magnetic tape, and all other removable data storage media.

## 4. STORAGE, TRANSMISSION AND DESTRUCTION OF PROTECTED HEALTH INFORMATION

All Protected Health Information will be rendered unusable, unreadable, or indecipherable to unauthorized individuals in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended and supplemented by the Health Information Technology for Economic and Public Health Act (HITECH). Without limiting the generality of the foregoing, Contractor will encrypt all workstations and portable devices (e.g., mobiles, wearables, tablets, thumb drives, external hard drives) that store County's Confidential Information (including Protected Health Information) in accordance with Federal Information Processing Standard (FIPS) 140-2. Contractor will encrypt County's Confidential Information transmitted on networks outside of Contractor's control with Secure Socket Layer (SSL or TLS), at a minimum, cipher strength of 256 bit. If County's Confidential Information is no longer required to be retained by Contractor under the Contract and applicable law, Contractor must destroy such information by: (a) shredding or otherwise destroying paper, film, or other hard copy media so that the information cannot be read or otherwise cannot be reconstructed; and (b) clearing, purging, or destroying electronic media containing Protected Health Information consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the Protected Health Information cannot be retrieved. Contractor will not store County's Confidential Information (including Protected Health Information) in the cloud or in any other online storage provider.

All mobile devices storing County's Confidential Information (including Protected Health Information) must be managed by a Mobile Device Management system. All workstations/PCs will maintain the latest security patches and have the latest virus definitions. Virus scans should be run daily and logged.

## 5. DATA CONTROL; MEDIA DISPOSAL AND SERVICING

Subject to and without limiting the requirements under Section 4 (Storage, Transmission and Destruction of Protected Health Information), Personally Identifiable Information, Protected Health Information, and County's Confidential Information: (i) may only be made available and accessible to those parties explicitly authorized under the Contract or otherwise expressly approved by the County in writing; (ii) if transferred across the Internet, any wireless network (e.g.,cellular, 802.11x, or similar technology), or other public or shared networks, must be protected using appropriate encryption technology as designated or approved by County Project Director in writing; and (iii) if transferred using Removable Media (as defined above) must be sent via a bonded courier or protected using encryption technology designated by Contractor and previously approved by the County in writing. The foregoing requirements will apply to back-up data stored by Contractor at off-site facilities. In the event any hardware, storage media, or Removable Media must be disposed of or sent off-site for servicing, Contractor must ensure all County's Confidential Information, including Personally Identifiable Information and Protected Health Information, has been cleared, purged, or scrubbed from such hardware and/or media using industry best practices (e.g., NIST Special Publication 800-88, Guidelines for Media Sanitization).

## 6. HARDWARE RETURN

Upon termination or expiration of the Contract or at any time upon County's request, Contractor must return all hardware, if any, provided by the County containing Personally Identifiable Information, Protected Health Information, or County's Confidential Information to County. The Personally Identifiable Information, Protected Health Information, and County's Confidential Information should not be removed or altered in any way. The hardware should

be physically sealed and returned via a bonded courier or as otherwise directed by the County. In the event the hardware containing County's Confidential Information or Personally Identifiable Information is owned by Contractor or a third party, a notarized statement, detailing the destruction method used and the data sets involved, the date of destruction, and the company and/or individual who performed the destruction will be sent to a designated County security representative within 15 days of termination or expiration of the Contract or at any time upon the County's request. Contractor's destruction or erasure of Personal Information and Protected Health Information pursuant to this Section will be in compliance with industry Best Practices (e.g., NIST Special Publication 800-88, Guidelines for Media Sanitization).

## 7. PHYSICAL AND ENVIRONMENTAL SECURITY

Contractor facilities that process Personally Identifiable Information, Protected Health Information, or County's Confidential Information must be housed in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physically secure environment from unauthorized access, damage, and interference.

## 8. COMMUNICATIONS AND OPERATIONAL MANAGEMENT

Contractor must: (i) monitor and manage all of its information processing facilities, including without limitation, implementing operational procedures, change management and incident response procedures; (ii) deploy adequate anti-viral software and adequate back-up facilities to ensure essential business information can be promptly recovered in the event of a disaster or media failure; and (iii) ensure its operating procedures will be adequately documented and designed to protect information, computer media, and data from theft and unauthorized access.

## 9. ACCESS CONTROL

Contractor must implement formal procedures to control access to its systems, services, and data, including but not limited to, user account management procedures and the following controls:

a. Network access to both internal and external networked services will be controlled, including but not limited to, the use of properly configured firewalls,

b. Operating systems will be used to enforce access controls to computer resources including but not limited to, authentication, authorization, and event logging,

c. Applications will include access control to limit user access to information and application system functions, and

d. All systems will be monitored to detect deviation from access control policies and identify suspicious activity. Contractor will record, review and act upon all events in accordance with incident response policies set forth below.

## 10. SECURITY INCIDENT

A "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification or interference with system operations in an information system.

a. Contractor will promptly notify (but in no event more than 24 hours after the detection of a Security Incident) the designated County security contact by telephone and subsequently via written letter of any potential or actual security attacks or Security Incidents.

b. The notice must include the approximate date and time of the occurrence and a summary

of the relevant facts, including a description of measures being taken to address the occurrence. A Security Incident includes instances in which internal personnel access systems in excess of their user rights or use the systems inappropriately.

c. Contractor will provide a report of all Security Incidents noting the corrective actions taken to mitigate the Security Incidents. This will be provided via a written letter to the County security representative as part of Contractor's annual audit or as reasonably requested by County. The County or its third party designee may, but is not obligated, perform audits and security tests of Contractor's environment that may include, but are not limited to, interviews of relevant personnel, review of documentation, or technical inspection of systems, as they relate to the receipt, maintenance, use, retention, and authorized destruction of Personally Identifiable Information, Protected Health Information, and County's Confidential Information.

d. County reserves the right to view, upon request, summary results (i.e., the number of high, medium and low vulnerabilities) and related corrective action schedule for which Contractor has undertaken on its behalf to assess Contractor's own network security. If requested, copies of these summary results and corrective action schedules will be sent to the County security contact.

## 11. CONTRACTOR SELF AUDIT

As part of Contractor's annual audit or upon the County's request, Contractor will provide to the County a summary of: (1) the results of any security audits, security reviews, or other relevant audits listed below, conducted by Contractor or a third party; and (2) the corrective actions or modifications, if any, Contractor will implement in response to such audits.

Relevant audits conducted by Contractor as of the effective date must include:

a. ISO 27001:2013 (Information Security Management) or FDA's Quality System Regulation, etc. – Contractor-wide. A full recertification is conducted every three years with surveillance audits annually.

   (i) **External Audit** – Audit conducted by non-Contractor personnel, to assess Contractor's level of compliance to applicable regulations, standards, and contractual requirements.

   (ii) **Internal Audit** – Audit conducted by qualified Contractor Personnel (or contracted designee) not responsible for the area of review, of Contractor organizations, operations, processes, and procedures, to assess compliance to and effectiveness of Contractor's Quality System (CQS) in support of applicable regulations, standards, and requirements.

   (iii) **Supplier Audit** – Quality audit conducted by qualified Contractor Personnel (or contracted designee) of product and service suppliers contracted by Contractor for internal or Contractor client use.

   (iv) **Detailed findings** – are not published externally, but a summary of the report findings, and corrective actions, if any, will be made available to the County as provided above and the ISO certificate is published on Buck Consultants LLC.

b. SSAE-16 (formerly known as SAS -70 II) – As to the Hosting Services only:

   (i) Audit spans a full 12 months of operation and is produced annually.

   (ii) The resulting detailed report is available to County.

(iii) Detailed findings are not published externally, but a summary of the report findings, and corrective actions, if any, will be made available to County as provided above.

## 12. SECURITY AUDITS

In addition to the audits described in Section 11 (Contractor Self Audit), during the term of this Contract, County or its third-party designee may annually, or more frequently as agreed in writing by the parties, request a security audit of Contractor's data center and systems. The audit will take place at a mutually agreed time by the parties, but in no event on a date more than 90 Days from the date of the request by the County. The County's request for security audit will specify the areas (e.g., Administrative, Physical and Technical) that are subject to the audit and may include but not be limited to: physical controls, inspection, process reviews, policy reviews, evidence of external and internal vulnerability scans, evidence of code reviews, and evidence of system configuration and audit log reviews. The County will pay for all third-party costs associated with the audit. It is understood that summary data of the results must be filtered to remove the specific information of other Contractor customers such as IP address, server names, etc.

Contractor will cooperate with the County in the development of the scope and methodology for the audit, and the timing and implementation of the audit. Any of the County's regulators will have the same right upon request, to request an audit as described above. Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

## 13. CONFIDENTIALITY

a. **Confidential Information.** Contractor agrees that all information supplied by its affiliates and agents to the County including, without limitation: (a) any information relating to the County's customers, patients, business partners, or personnel, (b) Personally Identifiable Information (as defined below), and (c) any Protected Health Information under HIPAA and HITECH, will be deemed confidential and proprietary to the County, regardless of whether such information was disclosed intentionally or unintentionally or marked as "confidential" or "proprietary" ("Confidential Information"). To be deemed "Confidential Information," trade secrets and mask works must be plainly and prominently marked with restrictive legends.

b. **County Data**. All of County's Confidential Information, data, records and information of the County to which Contractor has access, or otherwise provided to Contractor under this Contract (County Data), is and will remain the property of the County and the County retains exclusive rights and ownership thereto. The County Data may not be used by Contractor for any purpose other than as required under this Contract, nor may such data or any part of such data be disclosed, sold, assigned, leased or otherwise disposed of to third parties by Contractor or commercially exploited or otherwise used by or on behalf of Contractor, its officers, directors, employees, or agents.

c. **Non-Exclusive Equitable Remedy**. Subject to the limitations and other applicable provisions set forth in the Contract, Contractor acknowledges and agrees that due to the unique nature of Confidential Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach or threatened breach may result in irreparable harm to the County, and therefore, that upon any such breach or any threat thereof, the County will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies either of them might have at law or equity. Any breach of this Section 13 (Confidentiality) will constitute a material breach of this

Contract and be grounds for immediate termination of this Contract in the exclusive discretion of the County.

d. **Personally Identifiable Information.** "Personally Identifiable Information" means any information that identifies a person, including but not limited to: name, address, email address, passwords, account numbers, social security numbers, credit card information, personal financial or healthcare information, personal preferences, demographic data, marketing data, credit data, or any other identification data. For the avoidance of doubt, Personally Identifiable Information includes, but not be limited to, all "nonpublic personal information," as defined under the Gramm-Leach-Bliley Act (15 United States Code ("U.S.C.") §6801 et seq.), Protected Health Information, and "Personally Identifiable Information" as that term is defined in EU Data Protection Directive (Directive 95/46/EEC) on the protection of individuals with regard to processing of personal data and the free movement of such data.

   i. **Personally Identifiable Information**. In connection with this Contract and performance of the services, Contractor may be provided or obtain, from the County or otherwise, Personally Identifiable Information pertaining to County's current and prospective personnel, directors and officers, agents, investors, patients, and customers and may need to process such Personally Identifiable Information and/or transfer it, all subject to the restrictions set forth in this Contract and otherwise in compliance with all applicable foreign and domestic laws and regulations for the sole purpose of performing the services.

   ii. **Treatment of Personally Identifiable Information**. Without limiting any other warranty or obligations specified in this Contract, and in particular the Confidentiality provisions of the Contract, during the term of this Contract and thereafter in perpetuity, Contractor will not gather, store, log, archive, use, or otherwise retain any Personally Identifiable Information in any manner and will not disclose, distribute, sell, share, rent, or otherwise retain any Personally Identifiable Information to any third party, except as expressly required to perform its obligations in this Contract or as Contractor may be expressly directed in advance in writing by the County. Contractor represents and warrants that Contractor will use and process Personally Identifiable Information only in compliance with (a) this Contract, (b) the County's then current privacy policy, and (c) all applicable local, state, and federal laws and regulations (including, but not limited to, current and future laws and regulations relating to spamming, privacy, confidentiality, data security, and consumer protection).

   iii. **Retention of Personally Identifiable Information**. Contractor will not retain any Personally Identifiable Information for any period longer than necessary for Contractor to fulfill its obligations under this Contract. As soon as Contractor no longer needs to retain such Personally Identifiable Information in order to perform its duties under this Contract, Contractor will promptly return or destroy or erase all originals and copies of such Personally Identifiable Information as required by this Contract.

e. **Return of Confidential Information**. On the County's written request or upon expiration or termination of this Contract for any reason, Contractor will promptly: (a) return or destroy, at the County's option, all originals and copies of all documents and materials it has received containing County's Confidential Information, (b) if return or destruction is not permissible under applicable law, continue to protect such information in accordance with the terms of this Contract, and (c) deliver or destroy, at the County's option, all originals and copies of all summaries, records, descriptions, modifications, negatives, drawings, adoptions and other documents or materials, whether in writing or in machine-

readable form, prepared by Contractor, prepared under its direction, or at its request, from the documents and materials referred to in Subsection 13 (a), and provide a notarized written statement to the County certifying that all documents and materials referred to in Subsections13 (a) and (b) above have been delivered to the County or destroyed, as requested by the County. On termination or expiration of this Contract, the County will return or destroy all Contractor's Confidential Information (excluding items licensed to the County hereunder or that are required for use of the Deliverables and/or the Software), at Contractor's option.

# ATTACHMENT C.4

# COMPLIANCE WITH DEPARTMENTAL ENCRYPTION REQUIREMENTS

# FOR

# DEFENSE AND LAW ENFORCEMENT SOLUTION

# ATTACHMENT C.4

# COMPLIANCE WITH DEPARTMENTAL ENCRYPTION REQUIREMENTS

Contractor is required to provide information about its encryption practices with respect to Personal Information, Protected Health Information, Medical Information and any other information described in Paragraph 18.3 (Protection of Electronic County Information - Data Encryption) of the Contract by completing this Attachment C.4. By signing this Attachment C.4, Contractor certifies that it will be in compliance with the Los Angeles County Board of Supervisors Policy 5.200 (Contractor Protection of Electronic County Information) upon the effective date and during the Term of the Contract.

| | | | DOCUMENTATION AVAILABLE | |
|---|---|---|---|---|
| **COMPLIANCE QUESTIONS** | **YES** | **NO** | **YES** | **NO** |
| 1) Will County data stored on your workstation(s) be encrypted? | ☐ | ☐ | ☐ | ☐ |
| 2) Will County data stored on your laptop(s) be encrypted? | ☐ | ☐ | ☐ | ☐ |
| 3) Will County data stored on removable media be encrypted? | ☐ | ☐ | ☐ | ☐ |
| 4) Will County data be encrypted when transmitted? | ☐ | ☐ | ☐ | ☐ |
| 5) Will Contractor maintain a copy of any validation/attestation reports generated by its encryption tools? | ☐ | ☐ | ☐ | ☐ |
| 6) Will County data be stored on remote servers*? **cloud storage, Software-as-a-Service or SaaS* | ☐ | ☐ | ☐ | ☐ |

_____
Official's Name

_____
Official's Title

_____
Official's Signature

# ATTACHMENT C.5

# DEPARTMENTAL APPLICATION SECURITY REQUIREMENTS

# FOR

# DEFENSE AND LAW ENFORCEMENT SOLUTION

## TABLE OF CONTENTS

## Introduction

**Security Requirements Goals and Objectives:**

The Application Security Requirements outlines the overall security requirements that need to be addressed for every software application deployed and/or used by the County of Los Angeles (County). These requirements apply to all County and externally hosted applications: County developed and third party developed applications.

These requirements include the overall security capabilities needed to support the business processes for County departments and agencies. At a minimum, these requirements will be used to track, test and monitor the overall System's security capabilities that must consistently be met throughout the Term of the Contract.

Requests for exceptions to any specific requirements within this requirement must be reviewed by the Departmental Information Security Officer (DISO) and approved by the Departmental management. The request should specifically state the scope of the exception, along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, and risk mitigation measures to be undertaken by the project. The Departmental management will review such requests, confer with the requesting project team and approve as appropriate.

**Application Name and Brief Description**:

_____

_____

_____

_____

_____

**Application Owner Name**

_____

**Application Owner Signature**

_____

**Departmental Information Security Officer (DISO) Name:**

_____

**DISO Signature**

| Section Number | Security Requirements | Meets RQMTS (Y/N) | Comments/ Indicate Any Compensating Controls if Requirement Not Met |
|---|---|---|---|
| **1.0** | **Secure Coding** | | |
| 1.1 | Comply with the County Application Secure Coding Standard. | | |
| **2.0** | **Software as a Service (SaaS), if applicable** | | |
| 2.1 | Comply with the County SaaS Security and Privacy Standard. | | |
| **3.0** | **Authentication (Login/Sign-on)** | | |
| 3.1 | Authentication mechanism uses password that meets the County Password Security Standard. | | |
| 3.2 | Authentication must take place over a secured/encrypted transport protocol (e.g., HTTPS). | | |
| 3.3 | Application login must be integrated with a central department and/or county authentication mechanism (e.g., AD). | | |
| 3.4 | System encrypts passwords before transmission. | | |
| 3.5 | Ensure passwords are "hashed and salted" before storage. | | |

| Section Number | Security Requirements | Meets RQMTS (Y/N) | Comments/ Indicate Any Compensating Controls if Requirement Not Met |
|---|---|---|---|
| 3.6 | For public facing applications, implement multi-factor authentication for applications with sensitive (e.g., password) and/or confidential information (e.g., PII, PHI). | | |
| **4.0** | **Authorization (Permissions)** | | |
| 4.1 | Users are associated with a well-defined set of roles and privileges. | | |
| 4.2 | Users accessing resources hold valid credentials to do so, for example:<br>• User interface (UI) only shows navigation to authorized functions<br>• Server side authorization checks for every function<br>• Server side checks do not solely rely on information provided by user. | | |
| 4.3 | Role and permission metadata is protected from replay or tampering by using one of the following:<br>• Tokens/tickets expires after a single use or after a brief period<br>• Standard authorization/authentication protocol (e.g., SAML, OAuth). | | |

| Section Number | Security Requirements | Meets RQMTS (Y/N) | Comments/ Indicate Any Compensating Controls if Requirement Not Met |
|---|---|---|---|
| **5.0** | **Configuration Management (Database and Application Configuration Security)** | | |
| 5.1 | Database Security: System restricts users from directly accessing the database. | | |
| 5.2 | Application Configuration stores (e.g., web.config, httpd.conf) are secured from unauthorized access and tampering (secure file access permissions). | | |
| 5.3 | Application/database connection credentials need to be encrypted in transit and in storage. | | |
| 5.4 | Application/database connection and service accounts must comply with least privilege principle (must not be database admin account). | | |
| **6.0** | **Data Security** | | |
| 6.1 | Sensitive (e.g., password) and/or confidential data (e.g., PII, PHI) at rest and in transit must be in an encrypted format (per Board of Supervisors Policy No.5.200). | | |

| Section Number | Security Requirements | Meets RQMTS (Y/N) | Comments/ Indicate Any Compensating Controls if Requirement Not Met |
|---|---|---|---|
| 6.2 | Provide database/file encryption for protection of sensitive data fields while the data is at rest (e.g., stored data). | | |
| **7.0** | **Audit Logging and Reporting** | | |
| 7.1 | Application provides audit reports such as configuration, user accounts, roles, and privileges. | | |
| 7.2 | Auditing and logging an event in the system must include, at a minimum:<br>• Successful and unsuccessful logons to application<br>• Security Configuration changes (e.g., add users, delete users, change roles/group permissions, etc.)<br>• Sensitive business transaction/functions (e.g., override approvals)<br>• All logged information is handled securely and protected as per its data classification | | |

| Section Number | Security Requirements | Meets RQMTS (Y/N) | Comments/ Indicate Any Compensating Controls if Requirement Not Met |
|---|---|---|---|
| 7.3 | The event parameters logged must include:<br>• User or system account ID<br>• Date/time stamp<br>• IP address<br>• Error/event code and type<br>• Type of transaction<br>• User device or peripheral device involved in transactions<br>• Outcome (success or failure) of the event | | |
| 7.4 | Audit logs must be compliant with the applicable retention schedule and regulatory requirements. | | |
| **8.0** | **Reference** | | |
| 8.1 | County Web Application Secure Coding Standards. | | |
| 8.2 | County Password Security Standard. | | |
| 8.3 | Database Security Standard. | | |
| 8.4 | County Windows Server Baseline Security Standard. | | |