EXHIBIT C

SERVICE LEVEL AGREEMENT

RECORDS MANAGEMENT SYSTEM (RMS)

TABLE OF CONTENTS

PARAGRAPH **PAGE**

1.0 GENERAL

This Exhibit C, Service Level Agreement (hereinafter SLA), sets forth the scope of, and Contractor's Service level commitment regarding the Maintenance and Support Services (M&S) for the Solution, including, but not limited to, M&S service levels for Hardware and Software support, correction of Deficiencies, warranties, and the County's remedies for Contractor's failure to meet the Service level commitment specified herein. This SLA is supplemental to the warranties and representations made in the Contract. Capitalized terms used in this SLA without definition will have the meanings given to such terms in the Contract.

2.0 SCOPE OF SERVICES

2.1 Description

Contractor must provide M&S services specified in the Contract and this SLA, as more fully described in Paragraph 2.2 (Definitions) below.

2.2 Definitions

Customer Support: Has the meaning specified in Paragraph 4.1 (Scope of Support) below.

Disaster: A catastrophic event that results in Downtime or disruption of the Production Environment at the primary data center, and requires Contractor to maintain an Active-Passive Disaster Recovery plan.

Disaster Recovery: A network configuration of independent nodes having the ability to replicate the RMS Solution for real-time data recovery across the primary and secondary data centers instantaneously, as further described in Paragraph 4.3 (Business Continuity Strategy (Disaster Recovery)) of this SLA.

Downtime: The period of time that the Solution cannot be accessed due to the System, or any component thereof, being inaccessible.

Incident: A circumstance or set of circumstances taken together, resulting in a failure to meet a Service level as required under this SLA and which can result in a Downtime credit.

Maintenance Services: Any goods or Services provided under the Contract for maintaining the Solution. This includes, but is not limited to:

a. Hardware Maintenance (e.g., Preventive Maintenance, and scheduled/ unscheduled equipment repairs or replacement), and
b. Software Maintenance (e.g., Preventive Maintenance, Software Upgrades, Updates, enhancements, patches, and other updates to the Solution Software, Solution Interface updates needed to maintain compatibility with the Solution, Solution security updates, and report design updates, as further outlined in Paragraph 3.0 (Maintenance Services) below.

Preventive Maintenance: The regular inspection, cleaning and replacement of System components in order to optimize System functionality and prevent any Unscheduled Downtime due to System failure.

Service Credits: Credits (or any other form of discount) to be applied to the applicable Service fees for Contractor's failure to timely resolve an Incident, or correct a Deficiency, including System Downtime.

Severity Level: The applicable Deficiency severity level assigned to each Incident, for purposes of correcting Deficiencies, as described in Paragraph 5.2 (Resolution of Deficiencies) below.

SLA (Service Level Agreement): Refers to this Exhibit C and describes Contractor's Service level commitment regarding System maintenance as required by the Contract and this SLA, including but not limited to, M&S Services, and any/all warranties specified in the Contract and/or this SLA.

Support Hours: Means 365/366 Days per year, 24 hours per Day, 7 Days per week, with no exceptions made for holidays.

Support Services: Contractor's provision to the County of Customer Support services and help-desk assistance, as applicable.

System Availability: Has the meaning specified in Paragraph 5.3 (Solution Availability Requirements) below.

System Performance: The performance of the System with respect to Response Time, System Availability and Disaster Recovery.

System Performance Requirements: The requirements for System Performance, as agreed-to by the parties, pursuant to Paragraph 5.3 (Solution Availability Requirements) below.

System Software: means all application Software and operating Software, and related Documentation, provided by Contractor to the County as part of the Solution and residing in the Solution environment, and does not include equipment firmware.

Total Monthly Time: The total number of minutes during a calendar month, excluding Scheduled Downtime.

3.0 MAINTENANCE SERVICES

3.1 As part of Solution Maintenance, Contractor must provide Maintenance Services for all System Hardware delivered by Contractor to the County, and the Application Software, Interfaces, and Third-Party Software provided by Contractor to the County, as applicable, all as part of the Solution (hereinafter "Maintenance Services"), as provided in this Paragraph 3.0.

3.2 Also, as part of Solution Maintenance, Contractor must provide Helpdesk support for all Contractor-provided System Software, including the Operating System, transaction processing layer, and database layer of the entire System, as applicable, as provided in this Paragraph 3.0.

3.3 Contractor must provide to the County a comprehensive program of scheduled Preventive Maintenance to ensure the County 24/7 uninterrupted availability of the Solution. The Preventive Maintenance program must include, but is not limited to:

a. Hardware Preventive Maintenance including, but not limited to: inspections, cleaning, testing and connectivity, etc.
b. Software Preventive Maintenance including, but not limited to: OS tuning, database tuning/compacting, error log reviews, error log purging, and security Software reviews, etc.

3.4 <u>System Hardware</u>

As part of Maintenance Services, Contractor must provide maintenance of the Solution's System Hardware infrastructure. Contractor must pass thru to the County all equipment warranties provided by the original equipment manufacturers at the point of sale. Contractor must repair, upgrade/replace, or oversee the repair,

upgrade or replacement of, all System Hardware components as needed throughout the entire Term of the Contract to comply with the Solution Requirements and the warranties specified herein in this SLA and throughout the Contract.

3.4.1 As part of Contractor's Hardware Maintenance services for all Contractor-provided Solution Hardware, Contractor must:

a. Inspect, clean, and test connectivity of all Hardware including connectivity between all redundant server nodes,
b. Utilize automated monitoring tools to monitor Records Management System (RMS) server operations at all installed sites, and report all Deficiencies to the RMS help-desk,
c. Agree with the County regarding the Severity Level of each identified Hardware Deficiency, and remedy the Deficiency in accordance with Paragraph 5.2 (Resolution of Deficiencies) below,
d. Provide technical support to administer and operate all System environments (e.g., Production, Training, Testing, and Business Continuity),
e. Periodically test the RMS to ensure all data and configurations are automatically replicating (system backup) to each of the server sites as part of the Software Preventive Maintenance program, and as prescribed in the Business Continuity Strategy, and
f. Annually test the System failover process. The County and Contractor must mutually agree on the appropriate date and time.

3.4.2 Technology Refresh

At the conclusion of the fifth year of the Contract following Final Acceptance, and every five years thereafter should the Contract be extended beyond the original Term, a Technology Refresh will occur for all on-premise hardware (if any). Contractor must provide to the County a refreshment strategy to ensure the RMS Solution will, at a minimum, meet the System performance requirements and ensure all virtual hardware, software, and associated operating systems are fully supported. At the sole discretion of the County Project Director, the Technology Refresh will be procured, delivered, and installed by Contractor as Optional Work, payable by the County utilizing Pool Dollars pursuant to Paragraph 3.3.4 (Optional Work) of the Contract. The actual date for the Hardware upgrade will be as negotiated by the parties.

3.5 Application Software

3.5.1 Contractor must provide periodic Software Updates ("Updates") to the Application Software to keep current with Contractor's technology standards, industry standards, and Federal and California state mandates, and to maintain compatibility with the Solution Requirements, and with Third-Party Software, upgrades, updates, patches, bug fixes, etc. Contractor must timely deliver all Software Updates to the County, in accordance with this SLA and in coordination with County Project Manager.

3.5.2 Without limiting the other provisions of the Contract including, without limitation, the provisions of this SLA, such Updates must be provided to the County at least twice every year, unless otherwise agreed-to by the County and Contractor. Contractor must notify the County, at least two weeks in advance, of all such updates to the Application Software prior to the anticipated installation date thereof. The County will assess impacts to its business processes, if any, and verify whether the updates were tested successfully. If so, Contractor must proceed with transitioning updates to the Production Environment. If not, Contractor must conduct additional testing, until the County verifies successful testing.

3.5.3 Notwithstanding, the County may choose at its sole discretion not to implement a particular Software Update. Contractor and the County will discuss the impacts and risks to the County, if any, for not implementing a particular Software Update. Contractor must roll back any Software Update to its prior version, as instructed by the County, when severe issues arise. Contractor must provide the County with a clearly defined configuration management plan (e.g., version control and source code control processes).

3.5.4 Contractor's provision and installation of Software Updates (as defined in Paragraph 3.5 of the Contract) to the Application Software and all Third-Party applications are provided as part of Contractor's annual M&S service delivery and will be at no additional cost to the County.

3.5.5 Any Updates necessary to remedy security problems in the System (e.g., closing "back doors" or other intrusion-related problems) must be provided promptly following Contractor's knowledge of such problems. The County must also be notified in writing within 24 hours of Contractor's knowledge of the existence of any intrusions or other security problems or breaches that

may affect the integrity of the System Data or any other County data, subject to the provisions specified in Paragraph 19.0 (Security) of the Contract.

3.5.6 Contractor must install all RMS Application software security patches not later than 14 Days from the time when Contractor is notified by either: 1) a Third-Party Software company, or 2) Department's data security office.

3.6. Solution Interfaces

Contractor must maintain and update all Solution Interfaces to remain compatible with all System Updates, as applicable. Contractor must maintain and update all Solution Interfaces to accommodate changes made to any interfaced external system which was outside the control of the County or Contractor.

3.7. Third-Party Software

3.7.1 As part of Maintenance Services, Contractor must provide Maintenance Services for all Third-Party Software included in all the RMS Environments for the Solution, including but not limited to Operating Software, transaction processing software, data software, virtualization software, report-writer Software, and other software installed in the Production Environments and Test/Train Environment that is not Contractor's Application Software. Contractor must update, upgrade, or replace these System Software components throughout the entire Term of the Contract to comply with the Solution Requirements and the warranties specified herein, and to support and be compatible with the Application Software including any Application Modification provided by Contractor under the Contract.

3.7.2 Contractor must provide updates to the System Software to keep current with Contractor's technology standards, industry standards, updates to the Application Software and other Application Modifications, all in coordination with County Project Manager.

3.7.3 Contractor must utilize automated software provisioning tools to perform remote software patches and install Version Releases, including security and Windows updates. Contractor must test all Third-Party Software updates to the Solution in the RMS Test Environment. The County will verify whether the updates were tested successfully. If so, Contractor must proceed with transitioning updates to all the RMS Environments. If not, Contractor must conduct additional testing, until the County verifies successful testing.

Contractor must roll back any Third-Party Software update to its prior Version, as instructed by the County, when severe issues arise.

3.7.4 Contractor must utilize industry-standard software configuration management tools for tracking and controlling changes in the Solution for all RMS environments.

3.7.5 All third-party security patches must be delivered and installed monthly or as available, as part of regular maintenance, or sooner upon request from County Project Manager or the Department's data security office.

3.7.6 Contractor must provide all Third-Party Software maintenance for both the primary and secondary data centers, monthly or as requested by the County, as part of regular maintenance.

3.7.7 Furthermore, any Third-Party Application that may be incorporated into the Solution by Contractor and become part of the Application Software will be subject to the same System Maintenance obligations and requirements as the Application Software components that are owned or are proprietary to, Contractor.

3.8 Additional Products

3.8.1 Maintenance Services additionally include maintaining compatibility of the System Software with any Additional Products that may be acquired by the County under the Contract as Optional Work. Contractor must provide price quotes as requested by Department for Additional Products. Additional Products will include the provision to the County of all accompanying/supporting Documentation at no additional cost.

3.8.2 Prior to the installation of any Additional Product or any update thereto, Contractor must test and ensure such Additional Product's compatibility with the then-current version of the System Software including, without limitation, service packs and security patches, promptly upon their release. The County will validate the testing.

3.9 System Availability

Unless agreed-to otherwise in advance by the County, Contractor must provide all Maintenance Services, including installation of Updates, with no Downtime. If

Downtime occurs, Paragraph 5.4 (Solution Availability and Credits) of this SLA will apply. In the event that System Maintenance is required, Contractor must ensure that, during any such System Maintenance, the System Availability requirements of the Contract are met and that the RMS Solution remains fully operational.

4.0 SUPPORT SERVICES

4.1 Scope of Support

Contractor's responsibilities for supporting the operation of the Solution (hereinafter "Support Services") must include responding to problems reported, and correcting Deficiencies as specified in this SLA. As part of its Support Services, Contractor must provide operational support for the Solution during Support Hours, which must include without limitation, the provision of a Contractor Customer Support desk to correct any failure of the Solution and to remedy Deficiencies in accordance with Paragraph 5.0 (Correction of Deficiencies) below, to ensure that the Solution operates in accordance with the specifications, including the Solution Requirements, warranties and other requirements set forth in the Contract. Contractor's Customer Support desk must be accessable via telephone, email, and/or a Contractor-maintained web-based customer support portal.

4.2 Customer Support

4.2.1 Requests for Customer Support will be submitted only by authorized County technical support staff (County's 'help-desk'). All requests for Customer Support must be tracked and maintained by Contractor in the Customer Support portal, using an automated trouble ticketing system. Contractor must respond with a plan for resolving each Deficiency and respond to County Project Manager within the applicable required timeframe specified in Paragraph 5.2.1 (Problem Correction Priorities) below, depending on the Severity Level of the Deficiency.

Contractor's Customer Support responsibilities must also include, but not be limited to, the following:

a. Providing County's help-desk with access to Contractor's Customer Support via toll-free telephone, email, and/or a dedicated web-based Customer Support portal.

b. Providing a toll-free telephone number for County staff to call any time during Support Hours, managed by a live operator to quickly connect County staff with the appropriate Contractor Customer Support personnel.

c. Access to Contractor's Customer Support via the web-based trouble-ticketing system or telephone. The trouble-ticketing system must provide the County with a simple method to submit, track, and update issues. Authorized County help-desk personnel must be provided an account, and training on the use of the automated trouble ticketing system.

d. Responding within the timeframes specified in Paragraph 5.2.1 (Problem Correction Priorities) below, depending on the Severity Level of the Deficiency.

e. Working with County Project Manager and County's technical support staff to correct Deficiencies, keeping such County personnel informed regarding Solution updates and scheduled timeframes, and ensuring that all scheduled Downtime maintenance windows are clearly communicated by Contractor, and the requirements of this SLA are met.

f. Informing the County at least two weeks in advance when the automated trouble ticketing system requires any scheduled Maintenance.

g. Working with County Project Manager and County-authorized technical staff to correct Deficiencies.

h. Informing County Project Manager and County's help-desk personnel of all pending Software Updates, including the scheduled timeframes for delivery to ensure 99.999% System Availability.

i. Providing all Software Updates necessary to keep the Solution compliant with FBI's Criminal Justice Information Services (CJIS), and federal and state mandates.

j. Maintaining all RMS Solution Documentation and computer-based training tools to align with all Software Upgrades and Updates delivered to the County, inclusive of all security Software, as applicable.

k. Triaging, diagnosing, and resolving all County-submitted Deficiencies based on severity and business impact. If Contractor proposes a solution for the Deficiency with a workaround, the County may reevaluate and escalate or downgrade the Severity Level of such Deficiency. Contractor must work with the County to ensure that each service ticket case is documented and diagnosed properly.

l. Each Deficiency must be tracked in Contractor's Customer Support ticketing system by, at minimum, the following:

   i. Severity Level in accordance with the definitions specified in Paragraph 5.2.1 (Problem Correction Priorities) below,
   ii. Date/time notified by the County,
   iii. Name of Contractor's service technician(s) or engineer(s),
   iv. Component and, if applicable, sub-component,
   v. Tracking number,
   vi. Description of problem including, if applicable, Solution Software version,
   vii. Root cause of problem,
   viii. Action(s) taken to resolve issue and/or to prevent recurrence,
   ix. History of actions taken by Contractor and County personnel (including any communication), and
   x. Date/time completed by Contractor and communicated to the County.

m. Monitoring the Solution for security breaches and reporting and coordinating resolution of any such security breaches with the County.

n. Installing all Software security patches as specified in Paragraph 3.5.6 above.

4.2.2 During the M&S period, Contractor's Project Manager must meet with County Project Manager on a regularly scheduled basis, minimally monthly. Meetings may be conducted in person at a County-designated location, or via web-conferencing, as mutually agreed-upon in advance by the parties. Contractor must provide the County with meeting agendas and presentation materials reflecting the most recent and accurate M&S activity which, at minimum, includes:

a. Service ticket activity from the prior month, including the age of each open service ticket,

b. Listing of service tickets resolved from the prior month, including the time duration it took Contractor to resolve,
c. Summary of Downtime, along with dates, times and location (if applicable), and
d. Database and/or transaction statistics, as applicable.

4.2.3 Contractor must provide User and Technical refresher training when requested by the County, pursuant to the Project Control Document's Training Plan. The topics to be covered during the session will be determined by the County and planned accordingly with Contractor.

4.2.4 Contractor must provide Service Credits to the County for: a) its failure to meet the response timeframes, and/or b) its failure to meet the resolution timeframes to correct any Major Deficiency as specified in Paragraph 5.0 (Correction of Deficiencies) and more specifically in Paragraph 5.3 (Solution Availability Requirements) below.

4.2.5 Contractor must evaluate RMS Solution enhancement suggestions, whether initiated by the County or Contractor, using Contractor's trouble ticketing system. Contractor must conduct a preliminary evaluation of the proposed enhancement within 30 Days and update the ticket with that preliminary evaluation. Contractor must use this information for product enhancement planning.

4.3 BUSINESS CONTINUITY STRATEGY (DISASTER RECOVERY)

As part of Support Services, Contractor must provide Disaster Recovery Services, including modifications to the Business Continuity Strategy in the PCD throughout the entire Contract Term.

Contractor must maintain and implement an agreed-upon Disaster Recovery environment to ensure that the Solution is not interrupted during a declared disaster. All requirements of the Contract, including those relating to, but not limited to, Disaster Recovery procedures, security, personnel due-diligence, and training, must be addressed in the Business Continuity Strategy.

Upon occurrence or declaration of a force majeure event, Contractor must provide the agreed-upon services outlined in the Business Continuity Strategy. Contractor will be subject to the following minimum Disaster Recovery requirements, which must be incorporated into the Business Continuity Strategy:

a. Contractor has complete responsibility for continuation of Service and restoration of the Solution, as applicable.
b. In the event of a force majeure declaration [see Paragraph 69.0 (Force Majeure) of the Contract], Contractor is required to maintain regular and consistent communication with the County regarding the outage, and steps needed to restore the System and the Solution.
c. Contractor must configure the Solution to immediately failover to the next available data center to ensure 99.999% availability instantaneous with the occurrence of a force majeure event.

5.0 CORRECTION OF DEFICIENCIES

5.1 Identification of Deficiencies

Deficiencies may be identified either by Contractor's use of its own monitoring tools or discovered by the County. Upon discovery of a Deficiency by the County, the County will report the Deficiency and its Severity Level to Contractor's Customer Support for resolution in accordance with this SLA. Upon discovery of a Deficiency by Contractor, Contractor will report the Deficiency to County Project Manager. Regardless of the Deficiency discovery source, Contractor must keep the County informed on all identified Deficiencies. The parties must mutually agree to assign the appropriate Severity Level to any Deficiency discovered by Contractor.

The Severity Level of a Deficiency will be assigned according to the Severity Level definitions set forth in Paragraph 5.2.1 (Problem Correction Priorities) of this SLA. Based on Contractor's proposed solution and/or workaround(s) for the Deficiency, the County may reevaluate, and escalate or downgrade the Severity Level of the Deficiency, pursuant to Paragraph 5.2.3 (Severity Level Adjustment) to this SLA.

5.2 Resolution of Deficiencies

5.2.1 Problem Correction Priorities

For each Deficiency reported by the County to Contractor, the County will assign the Severity Level to that Deficiency. For each Deficiency discovered by Contractor by its own problem monitoring system, Contractor will initially assign that Deficiency's Severity Level in consultation with the County.

Following a report of a Deficiency from the County, Contractor must respond back to the County within the prescribed “Service Response Timeframe” and resolve each such Deficiency within the specified “Service Resolution Time: as specified in the table below.

Following the report of a Deficiency by Contractor, Contractor must resolve each such Deficiency within the specified “Resolution Time” based on the Severity Level agreed-to by the parties.

Resolution times for correction of Deficiencies reported by the County will start tolling when the County first notifies Contractor of a Deficiency by telephone or as otherwise specified herein, including Contractor’s Customer Support, and will end when the County determines that the Deficiency has been resolved.

Conversely, resolution times for correction of Deficiencies reported by Contractor to the County will start tolling when Contractor first notifies the County of a Deficiency by telephone or as otherwise specified herein, including Contractor’s Customer Support, and will end when the County determines that the Deficiency has been resolved.

Severity Level	Description of Deficiency (any one of the following)	Service Response Timeframe	Service Resolution Time
1 Critical	**Critical Severity level 1:** The System or any component of the System is down (Unscheduled Downtime) or is effectively non-responsive or does not function at all, as determined by the County. There is no way to circumvent the problem; a significant number of County Users are affected. A production business system is inoperable. Severity level 1 renders the Software or a component of the Software inoperative, causes an ongoing interruption or unusable to the end User's activities, causes an unrecoverable loss or corruption of data.	30 minutes Credits for each 30min block thereafter an 'incident' 31-60 incident 1 61-90 Incident 2 etc *Each incident is added to Downtime Credits.	Resolve incident or formulate reasonable workaround within two consecutive hours Downtime Credits double for each hour thereafter an 'incident'.
2 Severe	**High – Severity Level 2**: A component of the Solution is not performing in accordance with the specifications, creating significant County business impact, its core functionality is not available, or one of System Requirements is not met, as determined by the County.	One hours Credits for each hour thereafter an 'incident' 02:01-3hrs Incident 1	Resolve incident or formulate reasonable workaround within four consecutive hours Credits double for each hour thereafter an 'incident'
3 Moderate	Moderate – Severity Level 3: A component of the Solution is not performing in accordance with the specifications but there is a reasonable workaround; there are unexpected results, moderate or minor operational impact, as determined by the County.	Six hours Credits for hour thereafter an 'incident'	Resolve incident within five consecutive days Credits commence on day six for each calendar thereafter, 8am-5pm thereafter an 'incident'

Severity Level	Description of Deficiency (any one of the following)	Service Response Timeframe	Service Resolution Time
4 Low	Low – Severity Level 4: This is a low impact problem and is not significant to operations or is cosmetic in nature as determined by the County.	Two days Credits for each business day 8a-5p thereafter an 'incident'	Next Version Release, or 180 calendar days, unless otherwise agreed-to by the County and Contractor Credits for each business day 8am-5pm thereafter an 'incident'

5.2.2 Problem Resolution Process

For any Deficiency reported by the County or discovered by Contractor, Contractor must immediately commence corrective action. Contractor must correct all Deficiencies within the resolution times specified above. Contractor must also immediately commence to develop a workaround or a fix for any Severity Level 1 or Severity Level 2 Deficiency (hereinafter "Major Deficiency"). The County and Contractor must agree on the Deficiency resolution, whether by a permanent solution or a temporary workaround, as determined by the County.

Contractor must provide the best level of effort to correct all Deficiencies and, in particular, Major Deficiencies, within the prescribed resolution times. In the event that Contractor fails to correct a Deficiency within the prescribed resolution time, Contractor must provide the County with a written or electronic report that includes a detailed explanation of the status of such Deficiency, preliminary actions taken, detailed mitigation plans and an estimated time for completing the correction of such Deficiency. This process will be repeated until the Deficiency is resolved, and the resolution is approved by County Project Manager. The parties will jointly cooperate during this period.

5.2.3 Severity Level Adjustment

The County may escalate or downgrade the Severity Level of a Deficiency if the Deficiency meets the definition of the Severity Level as escalated or downgraded. A Deficiency may also be mutually escalated by the County and Contractor if the Deficiency persists or reoccurs, as determined by County Project Manager. At the time the Deficiency is escalated or downgraded, an appropriate timeline will be applied for resolution of such Deficiency in accordance with Paragraph 5.2.1 (Problem Correction Priorities) above. Contractor may request an exception to the prescribed timeline when there are extenuating circumstances. Such request may or may not be granted at the sole discretion of County Project Manager.

If a workaround may be provided by Contractor for a Deficiency, the County and Contractor may agree to downgrade the Severity Level of such Deficiency until an agreed-upon date. If a permanent fix is not provided by such agreed-upon date, the County will have sole discretion to escalate the Severity Level back to the original Severity Level or higher, as provided herein.

5.3 Solution Availability Requirements

The Solution must meet the Solution availability requirements specified below, including, but not limited to, those relating to Major Deficiencies and System Availability, as further specified in this SLA and the Solution Requirements. All Solution Downtime will be deemed a Major Deficiency for the purpose of the correction of Deficiencies and other County remedies. All Major Deficiencies, for purposes of this Paragraph 5.3, will be considered Solution Downtime, and will be subject to the Service credits stated below.

5.4 Solution Availability and Credits

The Solution must be operational at 99.999% availability. Performance will be measured monthly. It is the responsibility of Contractor to present reports identifying compliance with this requirement. In the event Contractor fails to meet the availability requirements, Contractor must provide Service Credits to the County as follows:

System Availability (% of Service Month)	Service Response/Resolution and/or Downtime Range / Month	Service Credits (%of Monthly Fee for Applicable Service Month)
=> 99.9% and < 100%	0.00 – 1.00 hours	2.5%
=> 98.9% and < 99.9%	1.01 – 8.00 hours	10%
=> 97.9% and < 98.9%	8.01 –15.00 hours	20%
=> 95.9% and < 97.9%	15.01 – 29.00 hours	50%
=> 93.9% and < 95.9%	29.01 – 44.00 hours	75%
and < 93.9%	44.01 – 58.00 hours	Fee Waived for that Month

System Availability will be calculated as follows:

System Availability = (Total Monthly Hours required availability – Unscheduled Downtime) ÷ Total Monthly Time

EXAMPLES:

- Case #1: June has 720 hours; System was 'lights-out' for 8 minutes.

  8/60 = .134 hours Solution Downtime
  720 - .134=719.866 hours, System was 'Available'
  719.866 / 720 = .9998138 = 99.981% Availability (2.5% Svc Credits Assessed)

- Case #2: June has 720 hours; System had a reported Severity Level 2 Deficiency which required 4 hours to remedy.

  4 hours Solution Downtime
  720 - 4=716 hours, System was 'Available'
  716 / 720 = .9944 = 99.4% Availability (5% Svc Credits Assessed)

- Case #3: June has 720 hours; System has a reported Severity Level 2 Deficiency which required 6 hours to remedy.

  6 hours to remedy = 8 hours of Solution Downtime [4 hours + 4 hours (2 hours "doubled")]
  720 - 8=712 hours, System was 'Available'
  712 / 720 = .9889 = 98.8% Availability (20% Svc Credits Assessed)

- Case #4: June has 720 hours; System had a reported Severity Level 3 Deficiency, and Contractor took 10 hours to respond.

  10 hour response time = 2 hours of Delayed Response/Resolution
  720-2=718 hours, Delayed Service Response/Resolution
  718/720=.9972=99.7% (5% Svc Credits Assessed)

ATTACHMENT C.1

COUNTY – INFORMATION SECURITY AND PRIVACY REQUIREMENTS EXHIBIT

RECORDS MANAGEMENT SYSTEM (RMS)

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

The County of Los Angeles ("County") is committed to safeguarding the Integrity of the County systems, Data, Information and protecting the privacy rights of the individuals that it serves. This Information Security and Privacy Requirements Exhibit ("Exhibit") sets forth the County and Contractor's commitment and agreement to fulfill each of their 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 Exhibit 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 a minimum standard and are in addition to the requirements of the underlying base agreement between the County and Contractor (the "Contract") 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 Exhibit 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 Exhibit and the Contract, this Exhibit 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 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 Exhibit and the 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 Exhibit and the 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 will 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

Refer to Paragraph 18.0 (Confidentiality) of the Contract.

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 Exhibit will also apply to all Subcontractors and third parties. Contractor or third party will 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 Exhibit, 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 Exhibit; and (ii) Contractor will 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 Exhibit.

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 mobile, wearables, 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 the 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 the 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 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 will 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 will 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:
Jeffrey Aguilar
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 (DISO)
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 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 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 Exhibit, 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 18.0 (Confidentiality) 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

Refer to Paragraph 33.5 (Audit and Inspection, Information Security and Privacy Requirements) of the Contract.

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

ADDENDUM A: CONTRACTOR HARDWARE CONNECTING TO COUNTY SYSTEMS

Notwithstanding any other provisions in this Contract, Contractor must ensure the following provisions and security controls are established for any and all Systems or Hardware provided under this contract.

a. **Inventory:** Contractor must actively manage, including through inventory, tracking, loss prevention, replacement, updating, and correcting, all hardware devices covered under this Contract. Contractor must be able to provide such management records to the County at inception of the contract and anytime upon request.

b. **Access Control:** Contractor agrees to manage access to all Systems or Hardware covered under this Contract. This includes industry-standard management of administrative privileges including, but not limited to, maintaining an inventory of administrative privileges, changing default passwords, use of unique passwords for each individual accessing Systems or Hardware under this Contract, and minimizing the number of individuals with administrative privileges to those strictly necessary. Prior to effective date of this Contract, Contractor must document their access control plan for Systems or Hardware covered under this Contract and provide such plan to the Department Information Security Officer (DISO) who will consult with the County's Chief Information Security Officer (CISO) for review and approval. Contractor must modify and/or implement such plan as directed by the DISO and CISO.

c. **Operating System and Equipment Hygiene:** Contractor agrees to ensure that Systems or Hardware will be kept up to date, using only the most recent and supported operating systems, applications, and programs, including any patching or other solutions for vulnerabilities, within 90 Days of the release of such updates, upgrades, or patches. Contractor agrees to ensure that the operating system is configured to eliminate any unnecessary applications, services and programs. If for some reason Contractor cannot do so within 90 Days, Contractor must provide a Risk assessment to the Sheriff's Department, Departmental Information Security Officer (DISO).

d. **Vulnerability Management:** Contractor agrees to continuously acquire, assess, and take action to identify and remediate vulnerabilities within the Systems and Hardware covered under this Contract. If such vulnerabilities cannot be addressed, Contractor must provide a Risk assessment to the Department Information Security Officer (DISO) who will consult with the County's Chief Information Security Officer (CISO). The County's CISO must approve the Risk acceptance and Contractor accepts liability for Risks that result to the County for exploitation of any un-remediated vulnerabilities.

e. **Media Encryption:** Throughout the duration of this Contract, Contractor will encrypt all workstations, portable devices (e.g., mobile, wearables, tablets,) and removable media (e.g., portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) associated with Systems and Hardware provided under this Contract in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise required or approved by the Sheriff's Department DISO.

f. **Malware Protection:** Contractor will provide and maintain industry-standard endpoint antivirus and anti-malware protection on all Systems and Hardware as approved or required by the Department Information Security Officer (DISO) who will consult with the County's Chief Information Security Officer (CISO) to ensure provided hardware is free, and remains free of malware. Contractor agrees to provide the County documentation proving malware protection status upon request.

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

ADDENDUM C: APPLICATION SOURCE CODE REPOSITORY

Contractor shall 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") shall 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 document 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 County may download, install, and make full functional use of the delivered code as specified and intended.

ATTACHMENT C.2

DEPARTMENTAL INFORMATION SECURITY REQUIREMENTS

RECORDS MANAGEMENT SYSTEM (RMS)

ATTACHMENT C.2

DEPARTMENTAL INFORMATION SECURITY REQUIREMENTS

This Attachment C.2 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. 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 C.2 will constitute a material, non-curable breach of the Contract by Contractor, entitling 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 C.2, capitalized terms will 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 (collectively"**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), must 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 C.2, "**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 must be rendered unusable, unreadable, or indecipherable to unauthorized individuals in accordance with HIPAA, as amended and supplemented by the HITECH Act. Without limiting the generality of the foregoing, Contractor will encrypt all workstations and portable devices (e.g., mobile, 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 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 approved by County in writing. The foregoing requirements must 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 at any time upon County's request, Contractor must return all hardware, if any, provided by 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 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 fifteen (15) days of termination or expiration ofthe Contract or at any time upon County's request. Contractor's destruction or erasure of Personal

Information and Protected Health Information pursuant to this Section must 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 facilitiesto 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 must 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 must record, review and act upon all events inaccordance with incident response policies set forth below.

10. SECURITY INCIDENT

A "Security Incident" will mean 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 twenty-four (24) hours afterthe detection of a Security Incident) the designated County security contact by telephone andsubsequently 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 summaryof 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. 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 County's request, Contractor will provide to 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 (3)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 andeffectiveness of Contractor's Quality System ("CQS") in support of applicable regulations, standards, and requirements.

   (iii) **Supplier Audit** – Quality audit conducted by qualified Contractor Personnel (orcontracted 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 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 twelve (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 asprovided 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 ninety (90) days from the date of the request by County. 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 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. 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 must cooperate with 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 must 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 County's customers, patients, business partners, or personnel; (b) Personally Identifiable Information (as defined below); and (c) any Protected Health Information under The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and The Health Information Technology for Economic and Public Health Act (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 County to which Contractor has access, or otherwise provided to Contractor under this Contract ("County Data"), is and will remain the property of County and 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 County, and therefore, that upon any such breach or any threat thereof, 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" will mean 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 must include, 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 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 County. Contractor represents and warrants that Contractor will use and process Personally Identifiable Information only in compliance with (a) this Contract, (b) County's then current privacy policy, and (c) all applicable local, state, and federal laws and regulations (including, butnot 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.

e. **Return of Confidential Information**. On County's written request or upon expiration or termination of this Contract for any reason, Contractor will promptly: (a) return or destroy, at 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 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 County certifying that all documents and materials referred to in Subsections13(a) and (b) above have been delivered to County or destroyed, as requested by County. On termination or expiration of this Contract, County will return or destroy all Contractor's Confidential Information (excluding items licensed to County hereunder or that are required for use of the Deliverables and/or the Software), at Contractor's option.

ATTACHMENT C.3

COMPLIANCE WITH DEPARTMENTAL ENCRYPTION REQUIREMENTS

RECORDS MANAGEMENT SYSTEM (RMS)

ATTACHMENT C.3

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 19.3 (Protection of Electronic County Information - Data Encryption) of the Contract. By signing this Attachment C.3, Contractor certifies that it will be in compliance with the Los Angeles County Board of Supervisors Policy 5.200 (Contractor Protection of Electronic CountyInformation) 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.4

DEPARTMENTAL APPLICATION SECURITY REQUIREMENTS

RECORDS MANAGEMENT SYSTEM (RMS)

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. 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 terms of the resultant agreement.

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 (e.g., password) for applications with sensitive 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: • User interface (UI) only shows navigation to authorized functions • Server side authorization checks for every function • 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: • Tokens/tickets expires after a single use or after a brief period • 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 (i.e., must not be database admin account)		
6.0	**Data Security**		
6.1	Sensitive (e.g., password protected) and/or confidential data (e.g., PII, PHI) at rest and in transit must be in an encrypted format (i.e., in compliance with Board of Supervisors Policy No.5.200)		
6.2	Provide database/file encryption for protection of sensitive data fields while the data is at rest (e.g., stored data)		

Section Number	Security Requirements	Meets RQMTS (Y/N)	Comments/ Indicate Any Compensating Controls if Requirement Not Met
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: • Successful and unsuccessful logons to application • Security Configuration changes (add and delete users, change roles/group permissions, etc.) • Sensitive business transaction/functions (e.g., override approvals) • All logged information is handled securely and protected as per its data classification		
7.3	The event parameters logged must include: • User or system account ID • Date/time stamp • IP address • Error/event code and type • Type of transaction • User device or peripheral device involved in transactions • Outcome (success or failure) of the event		
7.4	Audit logs must be compliant with the applicable retention schedule and regulatory requirements		

Section Number	Security Requirements	Meets RQMTS (Y/N)	Comments/ Indicate Any Compensating Controls if Requirement Not Met
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		