SERVICE AGREEMENT

This Service Agreement ("Agreement") is dated_____, and is between E.J. Ward, Inc., a Nevada corporation, ("Contractor"), and the County of Fresno, a political subdivision of the State of California ("County").

Recitals

A. The County uses the Contractor's automated fuel management systems, software ("Fuel View"), and hardware ("Fuel Control Terminals") for comprehensive management of County-owned fuel sites assets, vehicles, data, and fuel-site related physical parts and repair services.

B. The Contractor is the sole proprietary developer and owner of the integrated fuel management platform, including the Fuel View Software as a Service hosting environment and integrated Fuel Control Terminals. The Contractor provides all software, hardware, and system support either directly or through its authorized service network.

C. The County requires access to and continued use of Fuel View, now available as Software as a Service ("SaaS") cloud-hosted platform and solutions. The County will be provided with access to software updates and maintenance, secure data, call center support through the Contractor's Annual SaaS hosting subscription fees, and fuel-site related physical products and repair services as necessary.

D. The County's Purchasing Manual allows the County to utilize contracts that have been competitively bid by other governmental agencies and cooperative purchasing groups, including Sourcewell, a State of Minnesota local government agency and purchasing organization for public sector entities, to obtain preferential pricing.

E. The Contractor was awarded Sourcewell Master Agreement Contract No. 081524-EJW ("Cooperative Agreement"), which is made available by Sourcewell to its participating entities, and is based upon the Contractor's response to the Request for Proposal No. 081524 titled, 'Aboveground Fuel and Fluid Storage with Related Hardware, Software, and Services'.

F. The Contractor agrees to provide pricing to the County that is equivalent or better than the pricing offered under the Cooperative Agreement and agrees to abide by the terms as set forth within the Cooperative Agreement for the entirety of this Agreement.

G. The County and the Contractor now desire to execute this Agreement through the competitively bid terms of the Cooperative Agreement for SaaS cloud-hosted Fuel View software, updates and maintenance, call center support, and other fuel-site related parts and repair services.

The parties therefore agree as follows:

Article 1

Contractor's Responsibilities

1.1 **Scope of Services.** The Contractor shall perform all of the services provided in Exhibit A to this Agreement, titled "Scope of Services" and in accordance with the terms of the Cooperative Agreement.

1.2 **Representation.** The Contractor represents that it is qualified, ready, willing, and able to perform all of the services provided in this Agreement.

1.3 **Coordination of Work / Contractor Representative.** The Contractor shall coordinate all work with the County to minimize any interruptions to the normal operation of County operations, through the appointee as identified in section 2.1 of this Agreement. The Contractor shall provide a Contractor representative ("Contractor Representative") to represent the Contractor, who will work with the County to carry out the Contractor's obligations under this Agreement.

1.4 **Compliance with Laws.** The Contractor shall, at its own cost, comply with all applicable federal, state, and local laws and regulations in the performance of its obligations under this Agreement, including but not limited to workers compensation, labor, and confidentiality laws and regulations.

Article 2

County's Responsibilities

2.1 The County shall provide a County representative ("County Representative") to represent the County, who will work with the Contractor to carry out the Contractor's obligations under this Agreement. The County Representative for the County's General Services Department shall be the Fleet Services Manager, and/or their designee.

2.2 The County shall follow the Contractor's Fuel View (SaaS) & Parts terms as described in Exhibit A.

2.3 **County Obligations**. The County shall contact the Contractor on an as-needed basis to request services and/or physical products/hardware/interfacing devices, and as detailed in Exhibit A.

Article 3

Compensation, Invoices, and Payments

3.1 The County agrees to pay, and the Contractor agrees to receive, compensation for the performance of its services under this Agreement as described in Exhibit B to this Agreement, titled "Compensation."

3.2 **Maximum Compensation.** The maximum compensation payable to the Contractor under this Agreement is $585,000.00 for the initial three-year term of this Agreement. In the event this Agreement is extended for its first optional one-year extension ("Year 4"), the total compensation payable to the Contractor under this Agreement is $790,000.00. In the event this Agreement is extended for its final one-year extension ("Year 5"), the total compensation payable to the Contractor under this Agreement is $1,000,000. In the event the total maximum compensation amount in the Initial Term, Year 4, and/or Year 5 is not fully expended, the remaining unspent funding amounts shall roll over to each subsequent term's established maximum compensation.

The Contractor acknowledges that the County is a local government entity, and does so with notice that the County's powers are limited by the California Constitution and by State law, and with notice that the Contractor may receive compensation under this Agreement only for services performed according to the terms of this Agreement and while this Agreement is in effect, and subject to the maximum amount payable under this section. The Contractor further acknowledges that County employees have no authority to pay the Contractor except as expressly provided in this Agreement.

3.3 **Invoices.** The Contractor shall submit annual invoices for annual SaaS hosting subscription fees within 60 days after the subscription period begins. The Contractor shall

submit monthly invoices for all other services and related parts within 60 days after the month in which the Contractor performs services and in any case within 60 days after the end of the term or termination of this Agreement. All invoices shall reference the provided agreement number and be sent to the County of Fresno, General Services Department, Fleet Services, 4551 E. Hamilton Ave., Fresno, CA 93702, fleetservices@fresnocountyca.gov.

3.4 **Payment.** The County shall pay each correctly completed and timely submitted invoice within 45 days after receipt. The County shall remit any payment to the Contractor's address specified in the invoice.

3.5 **Incidental Expenses.** The Contractor is solely responsible for all of its costs and expenses that are not specified as payable by the County under this Agreement.

Article 4

Term of Agreement

4.1 **Term.** This Agreement is effective on May 1, 2026 and terminates on January 31, 2029, ("Initial Term"), except as provided in section 4.2, "Extension," or Article 6, "Termination and Suspension," below.

4.2 **Extension.** The term of this Agreement may be extended for no more than two, one-year periods only upon written approval of both parties at least 30 days before the first day of the next one-year extension period. The Director of General Services, or their designee, is authorized to sign the written approval on behalf of the County based on the Contractor's satisfactory performance. The extension of this Agreement by the County is not a waiver or compromise of any default or breach of this Agreement by the Contractor existing at the time of the extension whether or not known to the County.

Article 5

Notices

5.1 **Contact Information.** The persons and their addresses having authority to give and receive notices provided for or permitted under this Agreement include the following:

For the County:
Director of General Services
County of Fresno
333 W. Pontiac Way

Clovis, CA 93612
gsdcontracts@fresnocountyca.gov

For the Contractor:
Leslie Patterson
E.J. Ward, Inc.
12621 Silicon Drive, Suite 122,
San Antonio, TX 78249
patterson@ejward.com

5.2 **Change of Contact Information.** Either party may change the information in section 5.1 by giving notice as provided in section 5.3.

5.3 **Method of Delivery.** Each notice between the County and the Contractor provided for or permitted under this Agreement must be in writing, state that it is a notice provided under this Agreement, and be delivered either by personal service, by first-class United States mail, by an overnight commercial courier service, or by Portable Document Format (PDF) document attached to an email.

(A) A notice delivered by personal service is effective upon service to the recipient.

(B) A notice delivered by first-class United States mail is effective three County business days after deposit in the United States mail, postage prepaid, addressed to the recipient.

(C) A notice delivered by an overnight commercial courier service is effective one County business day after deposit with the overnight commercial courier service, delivery fees prepaid, with delivery instructions given for next day delivery, addressed to the recipient.

(D) A notice delivered by PDF document attached to an email is effective when transmission to the recipient is completed (but, if such transmission is completed outside of County business hours, then such delivery is deemed to be effective at the next beginning of a County business day), provided that the sender maintains a machine record of the completed transmission.

5.4 **Claims Presentation.** For all claims arising from or related to this Agreement, nothing in this Agreement establishes, waives, or modifies any claims presentation

requirements or procedures provided by law, including the Government Claims Act (Division 3.6 of Title 1 of the Government Code, beginning with section 810).

Article 6

Termination and Suspension

6.1 **Termination for Non-Allocation of Funds.** The terms of this Agreement are contingent on the approval of funds by the appropriating government agency. If sufficient funds are not allocated, then the County, upon at least 30 days' advance written notice to the Contractor, may:

(A) Modify the services provided by the Contractor under this Agreement; or

(B) Terminate this Agreement.

6.2 **Termination for Breach.**

(A) Upon determining that a breach (as defined in paragraph (C) below) has occurred, the County may give written notice of the breach to the Contractor. The written notice may suspend performance under this Agreement, and must provide at least 30 days for the Contractor to cure the breach.

(1) Remedies to Cure Breach:

a. Service Credits: The Contractor agrees to provide service credits to the County as compensation for any failure to meet the agreed-upon service expectations. The amount of service credits will be calculated based on the 99.95% uptime guarantee. For each 0.1% of downtime below the guarantee, a 10% service credit will be applied to the next month's bill.

(B) If the Contractor fails to cure the breach to the County's satisfaction within the time stated in the written notice, the County may terminate this Agreement immediately.

(C) For purposes of this section, a breach occurs when, in the determination of the County, the Contractor has:

(1) Obtained or used funds illegally or improperly;

(2) Failed to comply with any part of this Agreement;

(3) Submitted a substantially incorrect or incomplete report to the County; or

(4) Improperly performed any of its obligations under this Agreement.

6.3 **Termination without Cause.** In circumstances other than those set forth above, the County may terminate this Agreement by giving at least 30 days advance written notice to the Contractor.

6.4 **No Penalty or Further Obligation.** Any termination of this Agreement by the County under this Article 6 is without penalty to or further obligation of the County.

6.5 **County's Rights upon Termination.** Upon termination for breach under this Article 6, the County and the Contractor shall mutually agree upon the amount, if any, of monies disbursed under this Agreement that were not expended in compliance with the terms of this Agreement. The Contractor shall repay any such mutually agreed-upon amount within sixty (60) days of resolution. This section survives the termination of this Agreement.

6.6 **Disentanglement Obligations upon Termination.** At the County's discretion, upon expiration or termination of this Agreement, the Contractor shall accomplish a complete transition of the services as set forth in Exhibit A to the County, or to any replacement provider designated by the County, without any interruption of or adverse impact on the services. This process shall be referred to as "Disentanglement." The Contractor shall fully cooperate with the County, and/or any new service provider, and otherwise promptly take all steps, including, but not limited to providing to the County, or any new service provider, all requested information or documentation, required to assist the County in effecting a complete Disentanglement. The Contractor shall provide all information or documentation regarding the services, or as otherwise needed for Disentanglement, including, but not limited to: data conversion, client files, interface specifications, training staff assuming responsibility, passwords, and related professional services. The Contractor shall provide for the prompt and orderly conclusion of all work required under the Agreement, as the County may direct, including completion or partial completion of

projects, documentation of work in process, and other measures to assure an orderly transition to the County or the County's designee. All Contractor work done as part of the Disentanglement shall be performed by the Contractor and will be reimbursed by the County at no more than the Contractor's costs, not to exceed the maximum compensation paid, pursuant to Article 3 (Compensation, Invoices, and Payments) of this Agreement. The Contractor shall not receive any additional or different compensation for the work otherwise required by the Agreement. The Contractor's obligation to provide the services shall not cease until the County provides the Contractor written confirmation that the Disentanglement, including the performance by the Contractor of all asset-transfers and other obligations of the Contractor provided in this Section, is deemed satisfactorily completed by the County Representative.

Article 7

Independent Contractor

7.1 **Status.** In performing under this Agreement, the Contractor, including its officers, agents, employees, and volunteers, is at all times acting and performing as an independent contractor, in an independent capacity, and not as an officer, agent, servant, employee, joint venturer, partner, or associate of the County.

7.2 **Verifying Performance**. The County has no right to control, supervise, or direct the manner or method of the Contractor's performance under this Agreement, but the County may verify that the Contractor is performing according to the terms of this Agreement.

7.3 **Benefits**. Because of its status as an independent contractor, the Contractor has no right to employment rights or benefits available to County employees. The Contractor is solely responsible for providing to its own employees all employee benefits required by law. The Contractor shall save the County harmless from all matters relating to the payment of the Contractor's employees, including compliance with Social Security withholding and all related regulations.

7.4 **Services to Others.** The parties acknowledge that, during the term of this Agreement, the Contractor may provide services to others unrelated to the County.

Article 8

Indemnity and Defense

8.1 **Indemnity.** The Contractor shall indemnify and hold harmless and defend the County (including its officers, agents, employees, and volunteers) against all claims, demands, injuries, damages, costs, expenses (including attorney fees and costs), fines, penalties, and liabilities of any kind to the County, the Contractor, or any third party that arise from or relate to the performance or failure to perform by the Contractor (or any of its officers, agents, subcontractors, or employees) under this Agreement. The County may conduct or participate in its own defense without affecting the Contractor's obligation to indemnify and hold harmless or defend the County.

8.2 **Survival.** This Article 8 survives the termination of this Agreement.

Article 9

Insurance

9.1 The Contractor shall comply with all the insurance requirements in Exhibit D, titled "Insurance Requirements" to this Agreement.

Article 10

Ownership of Data

10.1 **Ownership of Data.** The parties acknowledge and agree that all the County's data (Data), is and shall remain the exclusive property of the County. The Contractor acknowledges that in performing its obligations under the Agreement it may have access to the County's networks and Data. The Contractor shall use and access such Data only as necessary for the purpose of providing the services and supporting the Software as agreed.

10.2 **Ownership of System Software.** The parties acknowledge and agree that, as between the Contractor and the County, title and full ownership of all rights in and to the System Software, System Documentation (as defined in Exhibit A), and all other materials provided to the County by the Contractor under the terms of this Agreement shall remain with the Contractor. The County will take reasonable steps to protect trade secrets (as defined in Government Code Section 7924.510(f)) of the System Software and System Documentation,

and which are identified as such by the Contractor. The County may not disclose or make available to third parties the System Software or System Documentation or any portion thereof, unless otherwise required by court order. The Contractor shall own all right, title and interest in and to all corrections, modifications, enhancements, programs, and work product conceived, created or developed, alone or with the County or others, as a result of or related to the performance of this Agreement, including all proprietary rights therein and based thereon. Except and to the extent expressly provided herein, the Contractor does not grant to the County any right or license, express or implied, in or to the System Software and System Documentation or any of the foregoing. The parties acknowledge and agree that, as between the Contractor and the County, full ownership of all rights in and to all County data, whether in magnetic or paper form, including without limitation printed output from the System, are the exclusive property of the County.

10.3 **Contractor Intellectual Property Rights.** The Contractor shall grant a non-exclusive, non-transferable, and non-perpetual license, at no additional cost, to the County to use the Contractor Products and Services to the extent allowed in the relevant Order or Scope of Work (SOW) as defined in Exhibit A (Permitted Use). The County may reproduce, modify or create derivative works for its own use, public display, and use any and all of the Contractor's copyrights in the homepage layout wireframe, sitemap, draft homepage design concept(s) interior page layouts (collectively, the "Contractor Designs") embodied in the County's website and intranet, which are prepared or caused to be prepared by the Contractor under this Agreement. All rights not licensed are reserved to the Contractor and no rights may be implied. The Contractor retains all intellectual property rights in the Software, and the County agrees to implement software protection measures designed to prevent unauthorized use and copying of the Software.

Article 11

Inspections, Audits, and Public Records

11.1 **Inspection of Documents.** The Contractor shall make available to the County, and the County may examine at any time during business hours and as often as the County deems

necessary, all of the Contractor's records and data with respect to the matters covered by this Agreement, excluding attorney-client privileged communications. The Contractor shall, upon request by the County, permit the County to audit and inspect all of such records and data to ensure the Contractor's compliance with the terms of this Agreement.

(A)The County may, at its sole discretion and with reasonable notice, conduct or commission audits of Contractor's security controls, systems, and procedures that store, process, or transmit County data to verify compliance with County IT security standards.

11.2 **State Audit Requirements.** If the compensation to be paid by the County under this Agreement exceeds $10,000, the Contractor is subject to the examination and audit of the California State Auditor, as provided in Government Code section 8546.7, for a period of three years after final payment under this Agreement. This section survives the termination of this Agreement.

11.3 **Public Records.** The County is not limited in any manner with respect to its public disclosure of this Agreement or any record or data that the Contractor may provide to the County. The County's public disclosure of this Agreement or any record or data that the Contractor may provide to the County may include but is not limited to the following:

(A) The County may voluntarily, or upon request by any member of the public or governmental agency, disclose this Agreement to the public or such governmental agency.

(B) The County may voluntarily, or upon request by any member of the public or governmental agency, disclose to the public or such governmental agency any record or data that the Contractor may provide to the County, unless such disclosure is prohibited by court order.

(C) This Agreement, and any record or data that the Contractor may provide to the County, is subject to public disclosure under the Ralph M. Brown Act (California Government Code, Title 5, Division 2, Part 1, Chapter 9, beginning with section 54950).

(D) This Agreement, and any record or data that the Contractor may provide to the County, is subject to public disclosure as a public record under the California Public

Records Act (California Government Code, Title 1, Division 10, Chapter 3, beginning with section 7920.200) ("CPRA").

(E) This Agreement, and any record or data that the Contractor may provide to the County, is subject to public disclosure as information concerning the conduct of the people's business of the State of California under California Constitution, Article 1, section 3, subdivision (b).

(F) Any marking of confidentiality or restricted access upon or otherwise made with respect to any record or data that the Contractor may provide *to* the County shall be disregarded and have no effect on the County's right or duty to disclose to the public or governmental agency any such record or data.

11.4 **Public Records Act Requests.** If the County receives a written or oral request under the CPRA to publicly disclose any record that is in the Contractor's possession or control, and which the County has a right, under any provision of this Agreement or applicable law, to possess or control, then the County may demand, in writing, that the Contractor deliver to the County, for purposes of public disclosure, the requested records that may be in the possession or control of the Contractor. Within five business days after the County's demand, the Contractor shall (a) deliver to the County all of the requested records that are in the Contractor's possession or control, together with a written statement that the Contractor, after conducting a diligent search, has produced all requested records that are in the Contractor's possession or control, or (b) provide to the County a written statement that the Contractor, after conducting a diligent search, does not possess or control any of the requested records. The Contractor shall cooperate with the County with respect to any County demand for such records. If the Contractor wishes to assert that any specific record or data is exempt from disclosure under the CPRA or other applicable law, it must deliver the record or data to the County and assert the exemption by citation to specific legal authority within the written statement that it provides to the County under this section. The Contractor's assertion of any exemption from disclosure is not binding on the County, but the County will give at least 10 days' advance written notice to the Contractor before disclosing any record subject to the Contractor's assertion of exemption

from disclosure. The Contractor shall indemnify the County for any court-ordered award of costs or attorney's fees under the CPRA that results from the Contractor's delay, claim of exemption, failure to produce any such records, or failure to cooperate with the County with respect to any County demand for any such records.

Article 12

Disclosure of Self-Dealing Transactions

12.1 **Applicability.** This Article 12 applies if the Contractor is operating as a corporation, or changes its status to operate as a corporation.

12.2 **Duty to Disclose.** If any member of the Contractor's board of directors is party to a self-dealing transaction, he or she shall disclose the transaction by completing and signing a "Self-Dealing Transaction Disclosure Form" (Exhibit C to this Agreement) and submitting it to the County before commencing the transaction or immediately after.

12.3 **Definition.** "Self-dealing transaction" means a transaction to which the Contractor is a party and in which one or more of its directors, as an individual, has a material financial interest.

Article 13

Confidentiality & Data Security

13.1 **Confidentiality.** The County and the Contractor may have access to information that the other considers to be a trade secret as defined in California Government Code section 7924.510(f).

13.2 Each party shall use the other's Information only to perform its obligations under, and for the purposes of, the Agreement. Neither party shall use the Information of the other Party for the benefit of a third party. Each Party shall maintain the confidentiality of all Information in the same manner in which it protects its own information of like kind, but in no event shall either Party take less than reasonable precautions to prevent the unauthorized disclosure or use of the Information.

13.3 The Contractor shall not disclose the County's data except to any third parties as necessary to operate the Contractor Products and Services (provided that the Contractor

hereby grants to the County, at no additional cost, a non-perpetual, noncancelable, worldwide, nonexclusive license to utilize any data, on an anonymous or aggregate basis only, that arises from the use of the Contractor Products and Services by the Contractor, whether disclosed on, subsequent to, or prior to the Effective Date, to improve the functionality of the Contractor Products and Services and any other legitimate business purpose, subject to all legal restrictions regarding the use and disclosure of such information).

(A) Contractor shall ensure all subcontractors or third parties with access to County data or systems are contractually obligated to comply with all applicable provisions of this Agreement, including the security, audit, and data ownership clauses. Contractor shall provide a list of such parties upon request.

13.4 Upon termination of the Agreement, or upon a Party's request, each Party shall return to the other all Information of the other in its possession. All provisions of the Agreement relating to confidentiality, ownership, and limitations of liability shall survive the termination of the Agreement.

13.5 All services performed by the Contractor shall be in strict conformance with all applicable Federal, State of California, and/or local laws and regulations relating to confidentiality, including but not limited to, California Civil Code, California Welfare and Institutions Code, California Health and Safety Code, California Code of Regulations, and the Code of Federal Regulations.

13.6 **Data Security.** The Contractor shall be responsible for the privacy and security safeguards, as identified in Exhibit E), entitled "Data Security." To the extent required to carry out the assessment and authorization process and continuous monitoring, to safeguard against threats and hazards to the security, integrity, and confidentiality of any County data collected and stored by the Contractor, the Contractor shall afford the County access as necessary at the Contractor's reasonable discretion, to the Contractor's facilities, installations, and technical capabilities. If new or unanticipated threats or hazards are discovered by either the County or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

(A) Multi-Factor Authentication (MFA) Requirement. All remote access by Contractor personnel or subcontractors to County systems or to any environment hosting County data shall be protected by multi-factor authentication (MFA) using a method compliant with NIST SP 800-63B standards.

(B) Encryption Standards. Contractor shall ensure that all County data is encrypted at rest using a minimum of AES-256 and encrypted in transit using TLS 1.2 or higher.

(C) The Contractor shall comply with all applicable Fresno County Information Technology Standards and Preferred Practices ("IT Standards"), Exhibit F to this Agreement, including but not limited to Sections 1.5 (Access Control), 1.6 (System Security Controls), and 1.7 (Security Auditing).

Article 14

General Terms

14.1 **Modification.** Except as provided in Article 6, "Termination and Suspension," this Agreement may not be modified, and no waiver is effective, except by written agreement signed by both parties. The Contractor acknowledges that County employees have no authority to modify this Agreement except as expressly provided in this Agreement.

14.2 **Non-Assignment.** Neither party may assign its rights or delegate its obligations under this Agreement without the prior written consent of the other party.

14.3 **Governing Law.** The laws of the State of California govern all matters arising from or related to this Agreement.

14.4 **Jurisdiction and Venue.** This Agreement is signed and performed in Fresno County, California. The Contractor consents to California jurisdiction for actions arising from or related to this Agreement, and, subject to the Government Claims Act, all such actions must be brought and maintained in Fresno County.

14.5 **Construction.** The final form of this Agreement is the result of the parties' combined efforts. If anything in this Agreement is found by a court of competent jurisdiction to be ambiguous, that ambiguity shall not be resolved by construing the terms of this Agreement against either party.

14.6 **Days.** Unless otherwise specified, “days” means calendar days.

14.7 **Headings.** The headings and section titles in this Agreement are for convenience only and are not part of this Agreement.

14.8 **Severability.** If anything in this Agreement is found by a court of competent jurisdiction to be unlawful or otherwise unenforceable, the balance of this Agreement remains in effect, and the parties shall make best efforts to replace the unlawful or unenforceable part of this Agreement with lawful and enforceable terms intended to accomplish the parties’ original intent.

14.9 **Nondiscrimination.** During the performance of this Agreement, the Contractor shall not unlawfully discriminate against any employee or applicant for employment, or recipient of services, because of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, military status or veteran status pursuant to all applicable State of California and federal statutes and regulation.

14.10 **No Waiver.** Payment, waiver, or discharge by the County of any liability or obligation of the Contractor under this Agreement on any one or more occasions is not a waiver of performance of any continuing or other obligation of the Contractor and does not prohibit enforcement by the County of any obligation on any other occasion.

14.11 **Entire Agreement.** This Agreement, including its exhibits, is the entire agreement between the Contractor and the County with respect to the subject matter of this Agreement, and it supersedes all previous negotiations, proposals, commitments, writings, advertisements, publications, and understandings of any nature unless those things are expressly included in this Agreement. If there is any inconsistency between the terms of this Agreement without its exhibits and the terms of the exhibits, then the inconsistency will be resolved by giving the following precedence order: (1) the text of this Agreement, excluding Exhibits A through F; (2) the text of the Cooperative Agreement; and then (3) the text of Exhibits A through F.

14.12 **No Third-Party Beneficiaries.** This Agreement does not and is not intended to create any rights or obligations for any person or entity except for the parties.

14.13 **Agent for Service of Process.** The Contractor represents to County that the Contractor's agent for service of process in California, and that such agent's address for receiving such service of process in California, which information the Contractor shall maintain with the office of the California Secretary of State, is as follows:

CT Corporation System

330 N Brand Blvd, Ste 700

Glendale, CA 91203

Los Angeles County

The Contractor further represents to the County that if the Contractor changes its agent for service of process in California, or the Contractor's agent for service of process in California changes its address for receiving such service of process in California, which changed information the Contractor shall maintain with the office of the California Secretary of State, the Contractor shall give the County written notice thereof within five (5) calendar days thereof pursuant to Article 5 of this Agreement.

14.14 **Authorized Signature.** The Contractor represents and warrants to the County that:

(A) The Contractor is duly authorized and empowered to sign and perform its obligations under this Agreement.

(B) The individual signing this Agreement on behalf of the Contractor is duly authorized to do so and his or her signature on this Agreement legally binds the Contractor to the terms of this Agreement.

14.15 **Electronic Signatures.** The parties agree that this Agreement may be executed by electronic signature as provided in this section.

(A) An "electronic signature" means any symbol or process intended by an individual signing this Agreement to represent their signature, including but not limited to (1) a digital signature; (2) a faxed version of an original handwritten signature; or (3) an electronically scanned and transmitted (for example by PDF document) version of an original handwritten signature.

(B) Each electronic signature affixed or attached to this Agreement (1) is deemed equivalent to a valid original handwritten signature of the person signing this Agreement for all purposes, including but not limited to evidentiary proof in any administrative or judicial proceeding, and (2) has the same force and effect as the valid original handwritten signature of that person.

(C) The provisions of this section satisfy the requirements of Civil Code section 1633.5, subdivision (b), in the Uniform Electronic Transaction Act (Civil Code, Division 3, Part 2, Title 2.5, beginning with section 1633.1).

(D) Each party using a digital signature represents that it has undertaken and satisfied the requirements of Government Code section 16.5, subdivision (a), paragraphs (1) through (5), and agrees that each other party may rely upon that representation.

(E) This Agreement is not conditioned upon the parties conducting the transactions under it by electronic means and either party may sign this Agreement with an original handwritten signature.

14.16 **Counterparts.** This Agreement may be signed in counterparts, each of which is an original, and all of which together constitute this Agreement.

[*SIGNATURE PAGE FOLLOWS*]

The parties are signing this Agreement on the date stated in the introductory clause.

E.J. Ward, Inc.

Markay Ward (Apr 1, 2026 12:02:41 CDT)
Markay R. Ward, President

12621 Silicon Dr #122
San Antonio, TX 78249

COUNTY OF FRESNO

Garry Bredefeld, Chairman of the Board
of Supervisors of the County of Fresno

Attest:
Bernice E. Seidel
Clerk of the Board of Supervisors
County of Fresno, State of California

By: _____
Deputy

For accounting use only:

Org No.: 8910
Account No.: 7309
Fund No.: 1000
Subclass.: 10000

Exhibit A

Scope of Services

The Contractor shall provide and perform all duties, responsibilities, and obligations set forth in this Agreement, and based on the Cooperative Agreement, located at https://www.sourcewell-mn.gov/cooperative-purchasing/081524-EJW, incorporated herein by reference as set forth herein.

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

Change Control Process: is defined as the process used by the County to inform County staff of new or updated production use systems.

Products and Services: is defined as the products and services made available to the County pursuant to this Agreement, which may include the Contractor's Products and Services accessible for use by the County on a subscription basis (e.g., SaaS), the Contractor's professional services, content from any professional services or other required equipment components or other required hardware, as specified in each Order or Scope of Work (SOW) (defined below).

License: is defined as the license granted under this Agreement, and the rights and obligations that it creates under the laws of the United States of America and the State of California, including without limitation, copyright and intellectual property law.

Order or SOW: a written order, proposal, or purchase document in which the Contractor agrees to provide, and the County agrees to purchase specific Contractor Products and Services. SOW") means a written order, proposal, or purchase document that is signed by both Parties and describes the Contractor Products and Services to be provided and/or performed by the Contractor. Each Order or SOW shall describe the Parties' performance obligations and any assumptions or contingencies associated with the implementations of the Contractor Products and Services, as specified in each Order or SOW placed hereunder.

Order Term: the then-current duration of performance identified on each Order or SOW, for which the Contractor has committed to provide, and the County has committed to pay for, the Contractor Products and Services.

Support: is defined as the ongoing support and maintenance services performed by the Contractor related to the Contractor Products and Services as specified in the Agreement.

System: is defined as the System Software and System Documentation, collectively, including all modifications and enhancements.

System Software: is defined as the Contractor's Products and Services provided and hosted by the Contractor. System Software does not include operating system software, or any other third-party software.

System Documentation: is defined as the documentation relating to the System Software, including all manuals, reports, brochures, sample runs, specifications, and other materials provided by the Contractor in connection with the System Software.

System Software Maintenance and Support: is defined as software hosting for System Software, regular software updates to System Software, and support provided for System Software in case of errors, mistakes, or other technical difficulties.

Malicious Code: is defined as any code, program, or sub-program the knowing or intended purpose or effect of which is to damage or maliciously interfere with the operation of software or any system such as the System or to halt, disable, or interfere with the operation of any software or system such as the System, or (ii) any device, method, or token that permits any person to circumvent without authorization the normal security of any software or system such as the System.

Acceptable Use Policy: means the Contractor's Acceptable Use Policy terms as of the date the County signs or submits an Order.

Business Day: means 8:00 a.m. - 5:00 p.m. Central Standard Time (CST), Monday through Friday, excluding federal public holidays in the United States.

Confidential Information: means all information disclosed by either party to the other, whether before or after the effective date of the Agreement that the recipient should reasonably understand to be confidential.

Distributor: means a third party appointed by the Contractor to distribute Products directly to customers subject to the terms and conditions imposed by their agreement.

EFT: means Electronic Fund Transfer.

Contractor Website: means website located at http://www.ejward.com.

Excessive: is defined for the purpose of this Agreement as time spent beyond what is considered industry acceptable, proper, usual, or necessary to solve the problem solely based on the judgment of the Contractor's Technical Support.

Exchange Policy: Exchange and/or repair of components is normally two to three (2-3) days after the receipt of the items in need of repair or exchange or after the receipt of a Return Material Authorization ("RMA"). A customer's exchange and shipment to the company must comply with the RMA policy found in the current published price book and reference a support ticket number assigned by the Contractor's Technical Support.

Force Majeure: is defined as an unforeseen or uncontrollable event including, without limitation, any act or provision of any present or future law or regulation or government authority, any act of God, pandemic, epidemic, war, civil or military disobedience or disorder, riot, terrorism, fire, earthquake, storm, flood, strike, work stoppage, or similar occurrence.

Onsite Labor: for the purpose of this Agreement is defined as a single technician's time spent at the hardware's location to troubleshoot, repair or replace defective components. It does not include travel time or mileage charges to and from the service call.

Overtime Rates: for the purpose of this Agreement are defined as charges equal to 1.5 times the base rate (preferred or otherwise) for work performed after normal business hours, on weekends or holidays. For work performed after normal business hours, weekends, or holidays invoiced at a minimum of four (4) hours, not inclusive of travel or other direct costs.

Preferred Rates: for the purpose of this Agreement are defined as those rates in the current published semi-annually Contractor price book using Sourcewell (formally National Joint Powers Alliance) or other similar cooperative group discounts.

Reseller: means a third party appointed by the Contractor to sell products, systems and solutions directly to customers subject to the terms and conditions imposed by their agreement.

Service Response vs Service Repair: means the Service Response requirements as defined in this Agreement. The actual time to Repair the equipment, however, cannot be

determined or controlled by the response time period. Each service call will require analysis to determine the failure, actual repair, and testing to confirm the unit is working within specifications. In special cases, the repair may require unique parts which require additional time to obtain.

Software as a Service: means Fuel View, SimplyFuel, and/or its Internet of Things (IoT) version hosted by the Contractor and deployed over the Internet rather than installed on a client's computer as of the date the County signs or submits an Order.

Third-Party Products: means third party software or products that the Contractor may provide to the County under this Agreement.

Third Party Hardware Support: means the Contractor agrees to provide customers with limited technical support in troubleshooting problems associated with "Third-Party" or "Non-Covered" hardware or software. The Contractor's Technical Support may consult with representatives of other support organizations if required. If the time required to resolve third party issues is excessive, customers will be contacted for authorization to proceed before charges are incurred.

Third Party Vendors: means an authorized reseller, certified service provider and other relationships that the Contractor established with certain commercial vendors.

User: means the County and County's employees, agents, contractors, or other users who obtain and use the Services from the Contractor (each such person or entity being a User).

2. **Warranties & Disclaimers.** The Contractor agrees that all services performed under this Agreement will materially conform in all aspects with the requirements of this Agreement and their specifications. The Contractor warrants that it takes all precautions that are standard in the industry, in California, to increase the likelihood of a successful performance for the Contractor's Products and Services.

Except as provided in herein provided, each Party hereby disclaims any and all other warranties of any nature whatsoever whether oral and written, express or implied, including, without limitation, the implied warranties of merchantability, title, non-infringement, and fitness for a particular purpose. The Contractor does not warrant that the Contractor's

Products and Services will meet the County's requirements.

3. **Documentation.** The Contractor shall provide to the County System Documentation, which shall consist of electronic media files. The electronic media files must be printable using PC software normally available at the County. The Contractor shall provide new System Documentation corresponding to all new Software Upgrades. The County may print additional copies of all documentation. All System Documentation is to be used by the County only for the purposes identified within this Agreement.

4. **Technical Information.** The Contractor shall provide technical information to the County. Such information may cover areas regarding the software discussed in this Agreement, third party software, and other matters considered relevant to the County by the Contractor. Technical information shall be provided at the discretion of the Contractor but will not be unreasonably withheld.

5. **Operating System Updates.** The application must run on a County operating system that is consistently and currently supported by the operating system vendor. No outdated or unsupported County operating system shall be implemented on the production network. The Contractor shall keep their software current in order to operate in this environment. Patches may include critical operating system updates and security patches.

6. **Adhere to Change Control Process.** The Contractor employs a procedure to implement updates, upgrades, and version releases to a system that is in production use. This forum allows the Contractor to inform the County of upcoming changes to a production system. The Contractor must inform the County a minimum of one week prior to any planned, non-emergency changes so that the Change Control Process may be followed.

7. **Storage and Sending.** If any services specified in this Agreement are used to store and/or send Confidential Information, the Contractor must be notified in writing, in advance of the storage or sending. Should the County provide such notice, the County must ensure that Confidential Information is stored behind a secure interface and that the Contractor Products and Services be used only to notify people of updates to the information that can be accessed after authentication against a secure interface managed by the County.

8. **Support Services.** Support Services are defined as technical support, account management, and inclusive of all other support offered under this Exhibit A, and the terms of any Order or SOW.

9. **Downtime.** Downtime shall be defined as System non-availability due to System Software error, malfunction, or due to System Software Maintenance and Support activity other than in accordance with the scheduling parameters set forth in this Agreement. Examples of Downtime include, without limitation, the County and public cannot access the System for reasons within the Contractor's control or any functional component of the System or interference is not available and is within the Contractor's control. The County requires that there be no unscheduled Downtime for routine System Software Maintenance and Support of the application Software. The County will accept occasional scheduled Downtime, not to exceed, four hours, for significant non-routine Updates and maintenance to be scheduled by the Contractor. Routine System Software Maintenance and Support includes such tasks as major System Software version Updates. The Contractor shall use its best efforts to keep scheduled Downtime for non-routine maintenance to a minimum (99.9% up time guarantee).

10. **Data Sources**. Data uploaded into the Contractor Products and Services must be brought in from County sources (interactions with end users and opt-in contact lists). The County cannot upload purchased contact information into the Contractor Products and Services without the Contractor's written permission and professional services support for list cleansing. The Contractor certifies that it will not sell, retain, use, or disclose any personal information provided by the County for any purpose other than retaining, using, or disclosing such personal information for the specific purpose of performing the services outlined within this Agreement.

11. **Passwords.** Passwords are not transferable to any third party. The County is responsible for keeping all passwords secure and all use of the Contractor products and services accessed through the County's passwords.

12. **Site Visit.** Contractor visits to County sites, as may be requested in writing by County, are available for reasons such as additional system training on hardware or software

usage and additional consultation on website services. Charges will be at the rates specified in Exhibit A and Exhibit B.

13. **County Feedback.** The County will provide feedback to the Contractor with any suggestion, enhancement, request, recommendation, correction or other feedback provided by the County relating to the use of the Contractor's Products and Services. The Contractor may use such submissions as it deems appropriate in its sole discretion

Contractor's Fuel View Software-as-a-Service (Saas) and Parts Terms

1. **SaaS Support Number**.

1-800-580-WARD (9273) or email support@ejward.com (email for non-emergency support only during normal business hours: Monday-Friday 8am-5pm CST).

2. **Contractor Obligations.**

For all Orders accepted by the Contractor and subject to this Agreement, the Contractor agrees to provide the Services and the applicable support listed on Orders, subject to and in accordance with the Contractor, its Fuel View, SaaS and Extended Warranty Agreement.

a) The Contractor shall provide immediate notification of any unauthorized use of the customer's account, issues that impact the security, stability and operational reliability of the customer's data and/or applications used to access the data.

b) Resolution times are as referenced under Exhibit A, 'Acceptable Use Policy Terms', section 4, titled 'Contractor Minimum Service Level Commitments'.

3. **County Obligations.**

The County agrees to:

a) pay when due the fees for the Services as described in section 3.4 of this Agreement;

b) use reasonable security precautions during use of the Services;

c) cooperate with Contractor's reasonable investigation of outages, security issues, and any suspected breach of the Agreement;

d) keep billing contact and other account information up to date;

e) General Services Department, Fleet Services Manager or their designee shall immediately notify the Contractor of any unauthorized use of the County's account or any other breach of the security of the Services;

f) pay all federal, state, and local sales, use, surcharges, excise, franchise, property, gross receipts, license, privilege, and any other taxes assessed with respect to the Services subject to any exemption; and

g) provide the Contractor with accurate factual information to help determine if any tax is due with respect to the provision of the Services, and if the Contractor is required by law to collect taxes on the provision of the Services, then the County must pay the Contractor the amount of the tax due or provide satisfactory evidence of the County's exemption from the tax.

4. **Acceptable Use Policy**

By agreeing to the terms and conditions of this Agreement, the County agrees to the Contractor's Acceptable Use Policy, as detailed in this Exhibit A.

5. **IP Numbers**

Contractor will maintain and control ownership of all Internet protocol numbers and addresses it may assign the County or request to be provided by the County. The Contractor may, upon written request and approval by the County, change or remove or request new Internet protocol numbers and addresses.

6. **Third-Party Products**

For the County's convenience, the Contractor may provide the County access to Third-Party Products through certain Third-Party Vendor relationships. Neither the Contractor nor any Third-Party Vendor makes any representations or warranties of any kind, express or implied, regarding any Third-Party Products.

a) The County agrees to observe the terms of any license or applicable end user subscriber agreement for Third-Party Products and the Contractor will not have any liability for the County's use of any Third-Party Products or any violation of any license agreements or end user subscriber agreements that govern such Third-Party

Products. The County will be solely responsible for any additional software of products that the County installs or uses in conjunction with the Services provided herein.

b) The County agrees to not:

i. copy any license keys or otherwise decrypt or circumvent any license key or,

ii. run Third-Party Products on a second system or through any other hosting provider, remove, modify, or obscure any copyright, trademark, or other proprietary rights notices that appear on or during use of any product provided by the Contractor, or reverse engineer, decompile, or disassemble any product provided under this agreement, except to the extent that such activity is expressly permitted by the Contractor in writing or applicable law.

7. **Operating System Licensing Terms**.

If Microsoft software is provided to the County as part of the Services, then additional restrictions may apply, including but not limited to limits on the number of authenticated users of the hosted environment unless expressly noted in an Order or SOW.

8. **Data Control and Location of Services.**

The method and means of providing the Services shall be under the exclusive control, management, and supervision of the Contractor giving due consideration to the requests of the County. The Services (including data storage) shall be provided solely from within the continental United States and on computing and data storage devices residing therein.

9. **Backup and Recovery of County Data.**

The County's data will be mirrored in real-time to the disaster recovery system. Data is backed up not less than hourly and backups are moved to an offsite long term storage multiple times a day. All data resides within the United States. A Service Level Commitment Agreement is provided under Exhibit A, 'Acceptable Use Policy Terms', section 4, titled 'Contractor Minimum Service Level Commitments'. A Recovery Point Objective of not more than seventy-two 72 hours for the system and application in a disaster is

in place. The Contractor shall test system failover quarterly and review its Business Continuity / Disaster Recovery Plan annually and with its critical vendors.

10. **Maintenance Periods / Application Updates.**

Unless as otherwise agreed to by the County on a case-by-case basis, the Contractor shall provide no less than three (3) calendar days prior notice to the County of all non-emergency maintenance or updates to be performed on the Services or application, such notice shall include a detailed description of all maintenance to be performed. For emergency maintenance, patches, critical bug fixes, the Contractor shall provide as much prior notice as commercially practicable to the County and shall provide a detailed description of all maintenance performed no greater than one (1) calendar day following the implementation of the emergency maintenance.

11. **Limitation of Liability and Indemnity Monitoring User Activity.**

Users voluntarily engage in the activity of Internet use and bear the risks associated with that activity. The Contractor exercises no control over and expressly disclaims any obligation to monitor its customers and other Users with respect to breaches of this Agreement or any content of the information made available for distribution via the Services, including without limitation any information passing through the Contractor's host computers, network hubs and points of presence, or the Internet, or any content posted any User may post on any server or website. In no event will the Contractor have any liability to the County or any third party for unauthorized access to, or alteration, theft, or destruction of information distributed or made available for distribution via the Services through the accident, or means attributable to County users.

12. **Warranty Disclaimer:**

Except as expressly set forth in this agreement, the services, including, without limitation, all information, content, and other services made available by the contractor or any third-party vendors, are provided on an "as is" or "as available" basis and neither the contractor makes any representations or warranties regarding the services. The contractor hereby disclaims any express or implied warranties and conditions of any kind or nature whatsoever, including,

without limitation, warranties related to any course of dealing, usage or trade practice, or implied warranties and conditions of merchantability or fitness for a particular purpose.

Except as expressly set forth in this agreement, the services, including, without limitation, all information, content, and other services made available by the Contractor or any third-party vendors are provided on an “as is” or “as available” basis and neither the Contractor makes any representations or warranties regarding the services. The Contractor hereby disclaims any express or implied warranties and conditions of any kind or nature whatsoever, including, without limitation, warranties related to any course of dealing, usage or trade practice, or implied warranties and conditions of merchantability or fitness for a particular purpose.

Exhibit A

Acceptable Use Policy Terms

These Acceptable Use Policy (the "AUP") terms govern the County's use of all Products and Services offered by the Contractor. These AUP terms apply to all Users.

1. **Prohibited Use.** The Contractor's services may only be used for lawful purposes. Users may not use the Services to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including:

a) Utilizing the Services to send mass unsolicited e-mail to third parties.

b) Utilizing the Services in connection with any illegal activity. Without limiting the general application of this provision, users may not: utilize the services to:

i. Copy material from third parties (including text, graphics, music, videos or other copyrightable material) without proper authorization;

ii. Misappropriate or infringe the patents, copyrights, trademarks, or other intellectual property rights of the Contractor or any third party;

iii. Violate any applicable state, federal and international law.

c) Utilizing the Services in connection with any tortious or actionable activity.

d) Utilizing the Services in connection with any other disruptive or abusive activity. Without limiting the general application of this provision, Users may not utilize the Services to:

i. Cause denial of service attacks against the Contractor or other network hosts or Internet users or to otherwise degrade or impair the operation of the services, facilities or the servers and or Internet users;

ii. Offer mail services, mail forwarding capabilities other than for the user's own account;

iii. Resell access to software installed on the Contractor's servers;

iv. Subvert, or assist others in subverting, the security or integrity of any systems, facilities or equipment;

v. Gain unauthorized access to the computer networks of the Contractor or any other person or customer;

vi. Provide passwords or access codes to persons not authorized to receive such materials by the operator of the system requiring the password or access code;

vii. Distribute or post any virus, worm, Trojan horse, or computer code intended to disrupt services, destroy data, or damage equipment, or disrupt the operation of the Services;

viii. Conduct port scans or other invasive procedures against any server;

ix. Post messages, run scripts or run software programs that consume excessive Computer Processing Unit ("CPU") time or storage space;

x. Use in any manner that might subject the Contractor to unfavorable regulatory action, subject the company to any liability for any reason, or adversely affect.

2. **Remedies.** Remedies include, but are not limited to:

a) Warning the User;

b) Removing the offending content;

c) Suspending the offending User from the Services;

d) Terminating the offending User from the Services;

e) Imposing fees or charges on the offending account in accordance with the applicable service contract; or

f) Taking other action in accordance with these AUP terms, the applicable this Agreement, and/or applicable law.

3. **Violations.** If the Contractor learns of a violation of these AUP terms, then the Contractor reserves the right to take any of the following actions, in accordance with the severity and duration of the violation:

a) Enforcement Actions. The Contractor will provide the County with at least 48

hours' notice (by email of otherwise) of any proposed suspension, restriction, limitation, modification, or termination of the Services or any functionality related to the Services based on an alleged violation of these AUP terms, this Agreement, or any other reason; provided, however, if (i) the County's violation of these AUP terms immediately threatens the security of or damages to the Contractor's network, information, data, software, hardware, or facilities or (ii) such suspension, restriction, limitation, modification, or termination is at the request of law enforcement or required by the appropriate legal authorities, then Contractor will give the County as much notice as is reasonably practicable under the circumstances. To the extent that any element or functionality of the Services, including, without limitation, a particular account or "server," is suspended, restricted, limited, modified, or terminated, the Contractor will use commercially reasonable efforts to minimize the effects against any other component or functionality of the Services.

b) Cooperation with Law Enforcement. The Contractor reserves the right to involve and cooperate with law enforcement or the appropriate legal authorities in investigations of claims of illegal activity involving its Services or any users thereof and to respond to any violations of these AUP terms to the extent permitted under applicable law. The County agrees that the Contractor is authorized to monitor communications into, and out of, its network facilities to prevent the introduction of viruses or other hostile code, to prevent intrusions, and to otherwise enforce the terms of these AUP terms. The County further agrees that the Contractor may disclose any and all of the County's information including, without limitation, assigned IP numbers, account history, and account use to any law enforcement agent who makes a written request, without further consent or notification to the County.

4. **Contractor Minimum Service Level Commitments**

Minimum Service Level Commitments			
Fuel View Applications (24x7x365)	SLA Coverage Time	Minimum Commitment	SLA Measurement Period
System Availability	24x7x365	99.95%	Monthly
Issue Response Time - Severity 1	24x7x365	30 minutes	Monthly
Issue Response Time - Severity 2	24x7x365	1 hour	Monthly
Issue Response Time - Severity 3	24x7x365	48 hours	Monthly
Issue Response Time - Severity 4	24x7x365	48 hours	Monthly
Non-Critical Applications (8am-5pm, Business Days)	SLA Coverage Time	Minimum Commitment	SLA Measurement Period
System Availability	8-5, Business Days	99.95%	Monthly
Issue Response Time - Severity 1	8-5, Business Days	30 minutes	Monthly
Issue Response Time - Severity 2	8-5, Business Days	1 hour	Monthly
Issue Response Time - Severity 3	8-5, Business Days	48 hours	Monthly
Issue Response Time - Severity 4	8-5, Business Days	48 hours	Monthly

SLA Metric	Metric Definition
"System Availability"	The System will be available to all Users in a Production environment and function as designed in accordance with System documentation.
"Response Time"	The Contractor will use commercially reasonable efforts to respond to each case within the applicable response time described in the table above, depending on the Severity Level set on the issue.
"Resolution Time"	The Contractor will use commercially reasonable efforts to resolve each case or provide a functioning work around within the applicable within the applicable resolution time described in the table above, depending on the Severity Level set on the issue.
"Severity 1"	The issue must be restored for business to continue. Critical job functions cannot be completed. (e.g., System down or unavailable and outage impacts many users)

"Severity 2"	The operations are severely affected. (e.g., disruption, access limitation, degraded performance issues, missing functionality, and/or "use-ability")
"Severity 3"	Little or non-business impact. Issues that are an enhancement request, or are cosmetic in nature, related to documentation (e.g., A functional error for which there is an acceptable workaround). System performance issue or bug affecting a small number of Users or minor function. Short-term workaround may be available.
"Severity 4"	Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting a small number of users. Reasonable workaround available. Resolution required as soon as reasonably practicable.
"Business Days"	The number of service days in a year excluding weekends and national holidays.
"Calendar Days"	The number of service days in a year, including weekends and national holidays.
Critical Application - Risk Methodology Non-Critical Application - Methodology	Availability Service Level & Issue Response/Resolution Metric The Available metric is defined at 99.95% of the time or more in any calendar month ("SLA"). Availability is defined as 24/7/365. The monthly measurement period will begin on the first Calendar Day of each month and end on the last Calendar Day of each month during the term of this Agreement. The final report for each month will be provided to the County by the 5th day of the month following each monthly measurement period.

Exhibit A

Contractor Parts & On-Site Support Terms

This section covers parts only, no labor, after initial Warranty expiration.

The County must contact the Contractor directly for all Support and On-site repair requests. If a User contacts a third-party service provider directly, the User shall be responsible for payment directly to the third party for all parts and services performed by the third-party provider, even if that provider is a local authorized or certified Contractor service and repair provider.

1. **Support.** System support will be provided as set forth in the following sections. The User will use the Contractors Support Number to report an issue. Service Requests are broken into one of two categories: (1) Phone support; or (2) local On-Site support:

   a) Phone support - Support Number: 1-800-580-WARD (9273) or email support@ejward.com (email for non- emergency support only during normal business hours: Monday-Friday 8am-5pm CST). The Contractor shall provide the User service call support on a 24 hour / 7-days per week basis.

   b) On-Site support: This service will be provided 24 hours by 7 days per week.

      i. On-site technician service will be approved after receipt of Purchase Order from “End User” unless request falls within the original Warranty expiration date of the Fuel Control Terminal.

      ii. On-site Emergency service after hours is available per the On-site Overtime Service Rates.

The Contractor will return the service call within the following time requirements:

   a) Within Four (4) hours to the number provided in the service request between the hours of 8 am-5 pm Monday - Friday Central Time; or

   b) Eight (8) hours to the number provided in the service request report during Evenings, Weekends and Federal Holidays.

2. Field Technician Contact Process: The Contractor’s call center operator will record each service request by ticket number and record the problem in writing. The operator will contact the on-call service technician. Should the on-call technician not be reached within

four (4) hours, the back-up on-call technician will be contacted. In the event, the back-up technician is not available; the National Service Manager will be contacted.

3. **Recorded Issues**. Recorded issues will be addressed in the following manner:

   a) Priority 1 – Requires immediate attention as performance is unreasonably degraded (i.e., the system is completely down). Every effort will be made to provide an immediate resolution.

   b) Priority 2 – Requires urgent action, as failures are extremely inconvenient (i.e., a site is down). Every effort will be made to provide a resolution as soon as possible.

   c) Priority 3 – Requires routine action, as failure is only somewhat inconvenient, resolution will be provided as soon as possible.

4. **Site Support.** On-site service within the following time requirements and limitations described will be provided:

   a) 12-24 hours if service request between the hours of 8 am & 5 pm Monday – Friday; or

   b) 24-48 hours if service request between the hours of 5:01 pm & 7:59 am Monday – Friday; or

   c) 24-48 hours if service request between the hours of 5:01 pm Friday & 7:59 am Monday; or

   d) 24-48 hours if service request occurred on any Local, State or Federal Holiday.

   e) Five (5) business days for locations with either:

      i. No local authorized service technician; or

      ii. Air travel is required to support the location

5. **Service Limitations.** The Contractor cannot be deemed non-compliant with Warranty or Support agreement requirements inclusive, but not limited to the following conditions:

a) Acts of God and Man-Made Events: Disruptions caused by heavy rains, earthquakes, flooding, tornadoes, lightning strikes, hurricanes, fires, snow, ice, sleet, or road closures and detours caused by Town, City or State construction projects where normal street or interstate traffic patterns to the County site are disrupted or stopped.

b) Pandemic or Similar Natural Events: Situations where technicians or contractors are denied access because of global, national or other local government regulations.

c) Non-access: Situations where the Contractor's technicians or its contractors are denied access to the fuel terminal sites due to locked fences, blocked passages, or no one answering the phone number provided to the service call operator.

d) Malicious Acts: Inclusive of but not limited to; vandalism, theft, gun shots, rock throwing, fire, and anywhere damage is not attributable to normal, fair wear and tear of hardware components.

e) Negligence: Inclusive of but not limited to; third party contractors hired by the "End User(s)" to perform fuel site maintenance that would impair the performance of the Contractor's equipment by disrupting electrical service or making non-authorized adjustments or modifications to the installed hardware or fuel control terminals.

f) Procedural Changes: Inclusive of but not limited to; the "End User(s)" changing the manner in which their employees interact with the fuel automation hardware. These changes may require systemic changes which are considered outside the normal software maintenance activities (i.e., operating systems "OS", business rules or software customization requests).

6. **Non-Contractor Equipment or Systems Failure.** Inclusive of but not limited to; the Contractor dispatching a technician and the cause of incident is found to be other than an agreement covered product. Standard current published pricing will apply for authorized repairs from that point forward.

7. **Examples of non-covered equipment inclusive of, but not limited to:**

Dispensers, Pumps and Pulsers	Vehicles or Fleet Assets
Tank Level Monitoring (TLS)	CANceiver, VIT, GPS, Cables
Electrical System	EM-Tag, Ring Antenna or Dongle
Network (TCP/IP), Switch, Wi-Fi Access Point, CAT 5 Cable, Routers, Bridges	All hardware & software versions of SFT, JettScan, or device Programmers
Customer Local Servers (Virtual or Physical)	Cards, Datakeys, Fobs, Encoders,
Cabinet, Base, Lock Assembly	Embossers, Printers
Hose Modules	

8. **Hardware Covered:** Included in this coverage are the hardware components of the Fuel Control Terminal ("FCT") that were installed as part of the Automated Fuel Management System ("AFMS") either by the Contractor, Technicians or a certified Contractor Technician.

a) Field modifications, additions or changes to the hardware without written authorization or approval by the Contractor may void this Agreement.

b) The Contractor is not liable if parts are no longer available due to end of life ("EOL") or not available from subcomponent suppliers for any hardware covered under this Agreement.

9. **Extent of Software Coverage:** The Contractor will ensure the proper operation of all the Contractor's copyrighted software programs and their interface to external programs previously installed directly by its employees.

10. **Software Covered:** Included in this coverage are the following Contractor copyrighted software programs installed on the primary cloud servers and backup system:

a) Fuel View Software, communication programs, listeners and parsers;

b) Database Interface Programs written by the Contractor;

c) Business Rule Operating Systems "OS"; and

d) Reports, Screens, Scripts and Data Files.

11. **Items Not Covered "Customer Hosted" Systems:** User supplied or third-party supplied software, computer or network equipment not specifically contracted for under this agreement.

Non-covered software and equipment include, but are not limited to:

a) Customers' local servers, laptop and desktop computer software and hardware

b) Support for customers' browsers, or printers

c) Customers' Local Network Management Hardware and Software

d) Third Party Software, and/or its OS and relational databases

It is the County's responsibility to update and maintain all patches and fixes for Third-Party software and databases.

12. **Third Party Software Support "SaaS" or "Customer Hosted" Systems:**

The Contractor agrees to provide at its sole discretion the County with limited technical support in resolving problems associated with Third-Party OS, databases, Virtual Private Network (VPN), and/or other network problems. The Contractor's Technical Support will consult with representatives of other support organizations as necessary.

If the time required to resolve external issues is excessive, "End User(s)" will be contacted for authorization to proceed prior to billing for this additional optional service.

13. **Vehicle Equipment**: The Contractor will provide phone support only for issues pertaining to Vehicle Mounted Equipment, Hose Module, EM-Tag, JettScan or SimplyFuel Tool.

On-site service and replacement of this equipment will be billed separately at the labor rates listed in the Cooperative Agreement.

14. **Miscellaneous Additional Conditions**: Additional equipment may be added to this agreement at any time; the age and condition of existing hardware will be taken into consideration. Repairs to existing hardware when required to qualify for addition to this Agreement, are based solely on the judgment of the Contractor and will be billed separately at the published labor rates and current published list price of parts. Future SaaS Support

Agreement costs will be adjusted to reflect additional equipment as needed. **Based solely on the judgment of the Contractor, the Contractor shall retain the exclusive right to refuse adding or may remove equipment from this agreement based on the equipment's serviceability.**

15. **Shipping**: The standard method of shipping is by Ground for this agreement.
    a) The County may request expedited shipments such as "Next Day" or "Two Day" for an additional cost.
    b) The Contractor shall retain the sole right to use those expedited methods to ensure system up time at its cost when the company determines such actions are warranted under this agreement and its use does not establish precedent for future shipments.

Exhibit B

Compensation

The Contractor will be compensated for Contractor's Products and Services under this Agreement as provided in this Exhibit B. The Contractor is not entitled to any compensation except as expressly provided in this Exhibit B. The total compensation payable to the Contractor under this Agreement is $1,000,000.

1. **SAAS Annual Fuel View Hosting and Support Fee** This annual upfront fee covers up to eighteen (18) existing Fuel Control Terminals and includes a new site located at 200 W Pontiac, Clovis, CA 93612. This subscription fee includes all standard services as detailed in Exhibit A, including all Fuel View upgrades, updates, maintenance, general support, and phone support as priced through the Cooperative Agreement.
2. **Fuel Site Repair and On-Site Support.** County requested services not covered under an existing warranty, will be provided at a discounted rate offered within the Cooperative Agreement.
3. **Fuel Site Related Parts and Supplies.** The Contractor shall provide physical goods and supplies at a twenty percent (20%) discount from current Manufacturer Suggested Retail Price List. This price list will be made available to County whenever updates and/or changes are made to the list.

TERM	DESCRIPTION	RATE
YEAR 1	SAAS FUEL VIEW HOSTING ANNUAL MAY 1, 2026, TO JANUARY 31, 2027	**$33,346.35**
YEAR 2	SAAS FUEL VIEW HOSTING ANNUAL FEBRUARY 1, 2027, TO JANUARY 31, 2028	**$45,836.90**
YEAR 3	SAAS FUEL VIEW HOSTING ANNUAL FEBRUARY 1, 2028, TO JANUARY 31, 2029	**$47,254.53**
YEAR 4 (OPTIONAL)	SAAS FUEL VIEW HOSTING ANNUAL FEBRUARY 1, 2029, TO JANUARY 31, 2030	**$49,741.61**
YEAR 5 (OPTIONAL)	SAAS FUEL VIEW HOSTING ANNUAL FEBRUARY 1, 2030, TO JANUARY 31, 2031	**$51,280.01**
	MAXIMUM TOTAL	**$227,459.40**

Exhibit C

Self-Dealing Transaction Disclosure Form

In order to conduct business with the County of Fresno ("County"), members of a contractor's board of directors ("County Contractor"), must disclose any self-dealing transactions that they are a party to while providing goods, performing services, or both for the County. A self-dealing transaction is defined below:

> "A self-dealing transaction means a transaction to which the corporation is a party and in which one or more of its directors has a material financial interest."

The definition above will be used for purposes of completing this disclosure form.

Instructions

(1) Enter board member's name, job title (if applicable), and date this disclosure is being made.

(2) Enter the board member's company/agency name and address.

(3) Describe in detail the nature of the self-dealing transaction that is being disclosed to the County. At a minimum, include a description of the following:

a. The name of the agency/company with which the corporation has the transaction; and

b. The nature of the material financial interest in the Corporation's transaction that the board member has.

(4) Describe in detail why the self-dealing transaction is appropriate based on applicable provisions of the Corporations Code.

The form must be signed by the board member that is involved in the self-dealing transaction described in Sections (3) and (4).

Exhibit C

(1) Company Board Member Information:			
Name:		**Date:**	
Job Title:			
(2) Company/Agency Name and Address:			
(3) Disclosure (Please describe the nature of the self-dealing transaction you are a party to)			
(4) Explain why this self-dealing transaction is consistent with the requirements of Corporations Code § 5233 (a)			
(5) Authorized Signature			
Signature:		Date:	

Exhibit D

Insurance Requirements

1. Required Policies

Without limiting the County's right to obtain indemnification from the Contractor or any third parties, the Contractor, at its sole expense, shall maintain in full force and effect the following insurance policies throughout the term of this Agreement.

(A) **Commercial General Liability.** Commercial general liability insurance with limits of not less than Two Million Dollars ($2,000,000) per occurrence and an annual aggregate of Four Million Dollars ($4,000,000). This policy must be issued on a per occurrence basis. Coverage must include products, completed operations, property damage, bodily injury, personal injury, and advertising injury. The Contractor shall obtain an endorsement to this policy naming the County of Fresno, its officers, agents, employees, and volunteers, individually and collectively, as additional insureds, but only insofar as the operations under this Agreement are concerned. Such coverage for additional insureds will apply as primary insurance and any other insurance, or self-insurance, maintained by the County is excess only and not contributing with insurance provided under the Contractor's policy.

(B) **Automobile Liability.** Automobile liability insurance with limits of not less than One Million Dollars ($1,000,000) per occurrence for bodily injury and for property damages. Coverage must include any auto used in connection with this Agreement.

(C) **Workers Compensation.** Workers compensation insurance as required by the laws of the State of California with statutory limits.

(D) **Employer's Liability.** Employer's liability insurance with limits of not less than One Million Dollars ($1,000,000) per occurrence for bodily injury and for disease.

(E) **Professional Liability.** Professional liability insurance with limits of not less than One Million Dollars ($1,000,000) per occurrence and an annual aggregate of Three Million Dollars ($3,000,000). If this is a claims-made policy, then (1) the retroactive date must be prior to the date on which services began under this Agreement; (2) the Contractor shall maintain the policy and provide to the County annual evidence of insurance for not less than five years after completion of services under this Agreement; and (3) if the policy is canceled or not renewed, and not replaced with another claims-made policy with a retroactive date prior to the date on which services begin under this Agreement, then the Contractor shall purchase extended reporting coverage on its claims-made policy for a minimum of five years after completion of services under this Agreement.

(F) **Technology Professional Liability (Errors and Omissions).** Technology professional liability (errors and omissions) insurance with limits of not less than Two Million Dollars ($2,000,000) per occurrence and in the aggregate. Coverage must encompass all of the Contractor's obligations under this Agreement, including but not limited to claims involving Cyber Risks.

(G) **Cyber Liability.** Cyber liability insurance with limits of not less than Two Million Dollars ($2,000,000) per occurrence. Coverage must include claims involving Cyber Risks. The cyber liability policy must be endorsed to cover the full replacement value of damage to, alteration of, loss of, or destruction of intangible property (including but not limited to information or data) that is in the care, custody, or control of the Contractor.

Definition of Cyber Risks. "Cyber Risks" include but are not limited to (i) Security Breach, which may include Disclosure of Personal Information to an Unauthorized Third Party; (ii) data breach; (iii) breach of any of the Contractor's obligations under Exhibit E of this Agreement; (iv) system failure; (v) data recovery; (vi) failure to timely disclose data breach or Security Breach; (vii) failure to comply with privacy policy; (viii) payment card liabilities and costs; (ix) infringement of intellectual property, including but not limited to infringement of copyright, trademark, and trade dress; (x) invasion of privacy, including release of private information; (xi) information theft; (xii) damage to or destruction or alteration of electronic information; (xiii) cyber extortion; (xiv) extortion related to the Contractor's obligations under this Agreement regarding electronic information, including Personal Information; (xv) fraudulent instruction; (xvi) funds transfer fraud; (xvii) telephone fraud; (xviii) network security; (xix) data breach response costs, including Security Breach response costs; (xx) regulatory fines and penalties related to the Contractor's obligations under this Agreement regarding electronic information, including Personal Information; and (xxi) credit monitoring expense.

2. Additional Requirements

(A) **Verification of Coverage.** Within 30 days after the Contractor signs this Agreement, and at any time during the term of this Agreement as requested by the County's Risk Manager or the County Administrative Office, the Contractor shall deliver, or cause its broker or producer to deliver, to the County Risk Manager, at 2220 Tulare Street, 16th Floor, Fresno, California 93721, or HRRiskManagement@fresnocountyca.gov, and by mail or email to the person identified to receive notices under this Agreement, certificates of insurance and endorsements for all of the coverages required under this Agreement.

(i.) Each insurance certificate must state that: (1) the insurance coverage has been obtained and is in full force; (2) the County, its officers, agents, employees, and volunteers are not responsible for any premiums on the policy; and (3) the Contractor has waived its right to recover from the County, its officers, agents, employees, and volunteers any amounts paid under any insurance policy required by this Agreement and that waiver does not invalidate the insurance policy.

(ii.) The commercial general liability insurance certificate must also state, and include an endorsement, that the County of Fresno, its officers, agents, employees, and volunteers, individually and collectively, are additional insureds insofar as the operations under this Agreement are concerned. The commercial general liability insurance certificate must also state that the coverage shall apply as primary insurance and any other insurance, or self-insurance, maintained by the County

shall be excess only and not contributing with insurance provided under the Contractor's policy.

(iii.) The automobile liability insurance certificate must state that the policy covers any auto used in connection with this Agreement.

(iv.) The professional liability insurance certificate, if it is a claims-made policy, must also state the retroactive date of the policy, which must be prior to the date on which services began under this Agreement.

(v.) The technology professional liability insurance certificate must also state that coverage encompasses all of the Contractor's obligations under this Agreement, including but not limited to claims involving Cyber Risks, as that term is defined in this Agreement.

(vi.) The cyber liability insurance certificate must also state that it is endorsed, and include an endorsement, to cover the full replacement value of damage to, alteration of, loss of, or destruction of intangible property (including but not limited to information or data) that is in the care, custody, or control of the Contractor.

(B) **Acceptability of Insurers.** All insurance policies required under this Agreement must be issued by admitted insurers licensed to do business in the State of California and possessing at all times during the term of this Agreement an A.M. Best, Inc. rating of no less than A: VII.

(C) **Notice of Cancellation or Change.** For each insurance policy required under this Agreement, the Contractor shall provide to the County, or ensure that the policy requires the insurer to provide to the County, written notice of any cancellation or change in the policy as required in this paragraph. For cancellation of the policy for nonpayment of premium, the Contractor shall, or shall cause the insurer to, provide written notice to the County not less than 10 days in advance of cancellation. For cancellation of the policy for any other reason, and for any other change to the policy, the Contractor shall, or shall cause the insurer to, provide written notice to the County not less than 30 days in advance of cancellation or change. The County in its sole discretion may determine that the failure of the Contractor or its insurer to timely provide a written notice required by this paragraph is a breach of this Agreement.

(D) **County's Entitlement to Greater Coverage.** If the Contractor has or obtains insurance with broader coverage, higher limits, or both, than what is required under this Agreement, then the County requires and is entitled to the broader coverage, higher limits, or both. To that end, the Contractor shall deliver, or cause its broker or producer to deliver, to the County's Risk Manager certificates of insurance and endorsements for all of the coverages that have such broader coverage, higher limits, or both, as required under this Agreement.

(E) **Waiver of Subrogation.** The Contractor waives any right to recover from the County, its officers, agents, employees, and volunteers any amounts paid under the policy of worker's compensation insurance required by this Agreement. The Contractor is solely responsible to obtain any policy endorsement that may be necessary to accomplish that waiver, but the Contractor's waiver of subrogation

under this paragraph is effective whether or not the Contractor obtains such an endorsement.

(F) **County's Remedy for Contractor's Failure to Maintain.** If the Contractor fails to keep in effect at all times any insurance coverage required under this Agreement, the County may, in addition to any other remedies it may have, suspend or terminate this Agreement upon the occurrence of that failure, or purchase such insurance coverage, and charge the cost of that coverage to the Contractor. The County may offset such charges against any amounts owed by the County to the Contractor under this Agreement.

(G) **Subcontractors.** The Contractor shall require and verify that all subcontractors used by the Contractor to provide services under this Agreement maintain insurance meeting all insurance requirements provided in this Agreement. This paragraph does not authorize the Contractor to provide services under this Agreement using subcontract.

Exhibit E

Data Security

A. Definitions.

Capitalized terms used in this Exhibit E have the meanings set forth in this section A.

"Authorized Employees" means the Contractor's employees who have access to Personal Information.

"Authorized Persons" means: (i) any and all Authorized Employees; and (ii) any and all of the Contractor's subcontractors, representatives, agents, outsourcers, and consultants, and providers of professional services to the Contractor, who have access to Personal Information and are bound by law or in writing by confidentiality obligations sufficient to protect Personal Information in accordance with the terms of this Exhibit E.

"Director" means the County's Chief Information Officer, or their designee.

"Disclose" or any derivative of that word means to disclose, release, transfer, disseminate, or otherwise provide access to or communicate all or any part of any Personal Information orally, in writing, or by electronic or any other means to any person.

"Person" means any natural person, corporation, partnership, limited liability company, firm, or association.

"Personal Information" means any and all information, including any data provided, or to which access is provided, to the Contractor by or upon the authorization of the County, including but not limited to vital records, that: (i) identifies, describes, or relates to, or is associated with, or is capable of being used to identify, describe, or relate to, or associate with, a person (including, without limitation, names, physical descriptions, signatures, addresses, telephone numbers, e-mail addresses, education, financial matters, employment history, and other unique identifiers, as well as statements made by or attributable to the person); (ii) is used or is capable of being used to authenticate a person (including, without limitation, employee identification numbers, government-issued identification numbers, passwords or personal identification numbers (PINs), financial account numbers, credit report information, answers to

security questions, and other personal identifiers); or is personal information within the meaning of California Civil Code section 1798.3, subdivision (a), or 1798.80, subdivision (e). Personal Information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

"Privacy Practices Complaint" means a complaint received by the County relating to the Contractor's (or any Authorized Person's) privacy practices, or alleging a Security Breach. Such complaint shall have sufficient detail to enable the Contractor to promptly investigate and take remedial action under this Exhibit E.

"Security Safeguards" means physical, technical, administrative or organizational security procedures and practices put in place by the Contractor (or any Authorized Persons) that relate to the protection of the security, confidentiality, value, or integrity of Personal Information. Security Safeguards shall satisfy the minimal requirements set forth in subsection C.(5) of this Exhibit E.

"Security Breach" means (i) any act or omission that compromises either the security, confidentiality, value, or integrity of any Personal Information or the Security Safeguards, or (ii) any unauthorized Use, Disclosure, or modification of, or any loss or destruction of, or any corruption of or damage to, any Personal Information.

"Use" or any derivative thereof means to receive, acquire, collect, apply, manipulate, employ, process, transmit, disseminate, access, store, disclose, or dispose of Personal Information.

B. Standard of Care.

(1) The Contractor acknowledges that, in the course of its engagement by the County under this Agreement, the Contractor, or any Authorized Persons, may Use Personal Information only as permitted in this Agreement.

(2) The Contractor acknowledges that Personal Information is deemed to be confidential information of, or owned by, the County (or persons from whom the County receives or has

received Personal Information) and is not confidential information of, or owned or by, the Contractor, or any Authorized Persons. The Contractor further acknowledges that all right, title, and interest in or to the Personal Information remains in the County (or persons from whom the County receives or has received Personal Information) regardless of the Contractor's, or any Authorized Person's, Use of that Personal Information.

(3) The Contractor agrees and covenants in favor of the County that the Contractor shall: (i) keep and maintain all Personal Information in strict confidence, using such degree of care under this Subsection B as is reasonable and appropriate to avoid a Security Breach; (ii) Use Personal Information exclusively for the purposes for which the Personal Information is made accessible to the Contractor pursuant to the terms of this Exhibit E; (iii) not Use, Disclose, sell, rent, license, or otherwise make available Personal Information for the Contractor's own purposes or for the benefit of anyone other than the County, without the County's express prior written consent, which the County may give or withhold in its sole and absolute discretion; and (iv) not, directly or indirectly, Disclose Personal Information to any person (an "Unauthorized Third Party") other than Authorized Persons pursuant to this Agreement, without the Director's express prior written consent.

Notwithstanding the foregoing paragraph, in any case in which the Contractor believes it, or any Authorized Person, is required to disclose Personal Information to government regulatory authorities, or pursuant to a legal proceeding, or otherwise as may be required by applicable law, the Contractor shall (a) immediately notify the County of the specific demand for, and legal authority for the disclosure, including providing the County with a copy of any notice, discovery demand, subpoena, or order, as applicable, received by the Contractor, or any Authorized Person, from any government regulatory authorities, or in relation to any legal proceeding, and (b) promptly notify the County before such Personal Information is offered by the Contractor for such disclosure so that the County may have sufficient time to obtain a court order or take any other action the County may deem necessary to protect the Personal Information from such

disclosure, and the Contractor shall cooperate with the County to minimize the scope of such disclosure of such Personal Information.

The Contractor shall remain liable to the County for the actions and omissions of any Unauthorized Third Party concerning its Use of such Personal Information as if they were the Contractor's own actions and omissions.

C. Information Security.

(1) The Contractor covenants, represents and warrants to the County that the Contractor's Use of Personal Information under this Agreement does and shall at all times comply with all federal, state, and local, privacy and data protection laws, as well as all other applicable regulations and directives, including but not limited to California Civil Code, Division 3, Part 4, Title 1.81 (beginning with section 1798.80), and the Song-Beverly Credit Card Act of 1971 (California Civil Code, Division 3, Part 4, Title 1.3, beginning with section 1747). If the Contractor Uses credit, debit, or other payment cardholder information, the Contractor shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing and maintaining all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the Contractor's sole cost and expense.

(2) The Contractor covenants, represents and warrants to the County that, as of the Effective Date, the Contractor has not received notice of any violation of any privacy or data protection laws, as well as any other applicable regulations or directives, and is not the subject of any pending legal action or investigation by, any government regulatory authority regarding same.

(3) Without limiting the Contractor's obligations under subsection C.(1) of this Exhibit E, the Contractor's (or Authorized Person's) Security Safeguards shall be no less rigorous than accepted industry practices and, at a minimum, include the following: (i) limiting Use of Personal

Information strictly to the Contractor's and Authorized Persons' technical and administrative personnel who are necessary for the Contractor's, or Authorized Persons', Use of the Personal Information pursuant to this Agreement; (ii) ensuring that all of the Contractor's connectivity to the County computing systems will only be through the County's security gateways and firewalls, and only through security procedures approved upon the express prior written consent of the Director; (iii) to the extent that they contain or provide access to Personal Information, (a) securing the Contractor's business facilities, data centers, paper files, servers, back-up systems and computing equipment, operating systems, and software applications, including, but not limited to, all mobile devices and other equipment, operating systems, and software applications with information storage capability; (b) employing adequate controls and data security measures with respect to the Contractor Facilities and Equipment), both internally and externally, to protect (1) the Personal Information from potential loss or misappropriation, or unauthorized Use, and (2) the County's operations from disruption and abuse; (c) having and maintaining network, device application, database and platform security; (d) maintaining authentication and access controls within media, computing equipment, operating systems, and software applications; and (e) installing and maintaining in all mobile, wireless, or handheld devices a secure internet connection, having continuously updated anti-virus software protection and a remote wipe feature always enabled, all of which is subject to express prior written consent of the Director; (iv) encrypting all Personal Information at advance encryption standards of Advanced Encryption Standards (AES) of 128 bit or higher (a) stored on any mobile devices, including but not limited to hard disks, portable storage devices, or remote installation, or (b) transmitted over public or wireless networks (the encrypted Personal Information must be subject to password or pass phrase, and be stored on a secure server and transferred by means of a Virtual Private Network (VPN) connection, or another type of secure connection, all of which is subject to express prior written consent of the Director); (v) strictly segregating

Personal Information from all other information of the Contractor, including any Authorized Person, or anyone with whom the Contractor or any Authorized Person deals so that Personal Information is not commingled with any other types of information; (vi) having a patch management process including installation of all operating system/software vendor security patches; (vii) maintaining appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks of Authorized Employees consistent with applicable law; (viii) providing appropriate privacy and information security training to Authorized Employees; and (ix) Contractor shall enforce user access controls aligned with NIST AC-2, AC-6, and audit all access under AU-2.

(4) During the term of each Authorized Employee's employment by the Contractor, the Contractor shall cause such Authorized Employees to abide strictly by the Contractor's obligations under this Exhibit E. The Contractor further agrees that it shall maintain a disciplinary process to address any unauthorized Use of Personal Information by any Authorized Employees.

(5) The Contractor shall, in a secure manner, backup daily, or more frequently if it is the Contractor's practice to do so more frequently, Personal Information received from the County, and the County shall have immediate, real time access, at all times, to such backups via a secure, remote access connection provided by the Contractor, through the Internet. Backup procedures must include daily integrity validation with County audit access on request.

(6) The Contractor shall provide the County with the name and contact information for each Authorized Employee (including such Authorized Employee's work shift, and at least one alternate Authorized Employee for each Authorized Employee during such work shift) who shall serve as the County's primary security contact with the Contractor and shall be available to assist the County 24 hours per day, seven days per week as a contact in resolving the Contractor's and any Authorized Persons' obligations associated with a Security Breach or a Privacy Practices Complaint.

D. Security Breach Procedures.

(1) Within 24 hours of breach confirmation the Contractor shall (a) notify the Director of the Security Breach, such notice to be given first by telephone at the following telephone number, followed promptly by email at the following email address: (559) 600-5900 fresnocounty@service-now.com (which telephone number and email address the County may update by providing notice to the Contractor), and (b) preserve all relevant evidence (and cause any affected Authorized Person to preserve all relevant evidence) relating to the Security Breach. The notification shall include, to the extent reasonably possible, the identification of each type and the extent of Personal Information that has been, or is reasonably believed to have been, breached, including but not limited to, compromised, or subjected to unauthorized Use, Disclosure, or modification, or any loss or destruction, corruption, or damage.

(2) Immediately following the Contractor's notification to the County of a Security Breach, as provided pursuant to subsection D(1) of this Exhibit E, the Parties shall coordinate with each other to investigate the Security Breach. The Contractor agrees to fully cooperate with the County, including, without limitation: (i) assisting the County in conducting any investigation; (ii) providing the County with physical access to the facilities and operations affected; (iii) facilitating interviews with Authorized Persons and any of the Contractor's other employees knowledgeable of the matter; and (iv) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by the County. To that end, the Contractor shall, with respect to a Security Breach, be solely responsible, at its cost, for all notifications required by law and regulation, and the Contractor shall provide a written report of the investigation and reporting required to the Director within 30 days after the Contractor's discovery of the Security Breach.

(3) The County shall promptly notify the Contractor of the Director's knowledge, or reasonable belief, of any Privacy Practices Complaint, and upon the Contractor's receipt of notification thereof, the Contractor shall promptly address such Privacy Practices Complaint,

including taking any corrective action under this Exhibit E, all at the Contractor's sole expense, in accordance with applicable privacy rights, laws, regulations and standards. In the event the Contractor discovers a Security Breach, the Contractor shall treat the Privacy Practices Complaint as a Security Breach. Within 24 hours of the Contractor's receipt of notification of such Privacy Practices Complaint, the Contractor shall notify the County whether the matter is a Security Breach, or otherwise has been corrected and the manner of correction, or determined not to require corrective action and the reason therefor.

(4) The Contractor shall take prompt corrective action to respond to and remedy any Security Breach and take reasonable mitigating actions, including but not limiting to, preventing any reoccurrence of the Security Breach and correcting any deficiency in Security Safeguards as a result of such incident, all at the Contractor's sole expense, in accordance with applicable privacy rights, laws, regulations and standards. The Contractor shall reimburse the County for all reasonable costs incurred by the County in responding to, and mitigating damages caused by, any Security Breach, including all costs of the County incurred in relation to any litigation or other action described in subsection D.(5) of this Exhibit E to the extent applicable: (1) the cost of providing affected individuals with credit monitoring services for a specific period not to exceed 12 months, to the extent the incident could lead to a compromise of the data subject's credit or credit standing; (2) call center support for such affected individuals for a specific period not to exceed 30 days; and (3) the cost of any measures required under applicable laws.

E. Oversight of Security Compliance.

(1) The Contractor shall have and maintain a written information security policy that specifies Security Safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities.

(2) Upon the County's written request, to confirm the Contractor's compliance with this Exhibit E, as well as any applicable laws, regulations and industry standards, the Contractor grants the County or, upon the County's election, a third party on the County's behalf,

permission to perform an assessment, audit, examination or review of all controls in the Contractor's physical and technical environment in relation to all Personal Information that is Used by the Contractor pursuant to this Agreement. The Contractor shall fully cooperate with such assessment, audit or examination, as applicable, by providing the County or the third party on the County's behalf, access to all Authorized Employees and other knowledgeable personnel, physical premises, documentation, infrastructure and application software that is Used by the Contractor for Personal Information pursuant to this Agreement. In addition, the Contractor shall provide the County with the results of any audit by or on behalf of the Contractor that assesses the effectiveness of the Contractor's information security program as relevant to the security and confidentiality of Personal Information Used by the Contractor or Authorized Persons during the course of this Agreement under this Exhibit E.

(3) The Contractor shall ensure that all Authorized Persons who Use Personal Information agree to the same restrictions and conditions in this Exhibit E. that apply to the Contractor with respect to such Personal Information by incorporating the relevant provisions of these provisions into a valid and binding written agreement between the Contractor and such Authorized Persons, or amending any written agreements to provide same.

F. Return or Destruction of Personal Information.

Upon the termination of this Agreement, the Contractor shall, and shall instruct all Authorized Persons to, promptly return to the County all Personal Information, whether in written, electronic or other form or media, in its possession or the possession of such Authorized Persons, in a machine readable form used by the County at the time of such return, or upon the express prior written consent of the Director, securely destroy all such Personal Information, and certify in writing to the County that such Personal Information have been returned to the County or disposed of securely, as applicable. If the Contractor is authorized to dispose of any such Personal Information, as provided in this Exhibit E, such certification shall state the date, time, and manner (including standard) of disposal and by whom, specifying the title of the

individual. The Contractor shall comply with all reasonable directions provided by the Director with respect to the return or disposal of Personal Information and copies thereof. If return or disposal of such Personal Information or copies of Personal Information is not feasible, the Contractor shall notify the County accordingly, specifying the reason, and continue to extend the protections of this Exhibit E to all such Personal Information and copies of Personal Information. The Contractor shall not retain any copy of any Personal Information after returning or disposing of Personal Information as required by this section F. The Contractor's obligations under this section F survive the termination of this Agreement and apply to all Personal Information that the Contractor retains if return or disposal is not feasible and to all Personal Information that the Contractor may later discover.

G. Equitable Relief.

The Contractor acknowledges that any breach of its covenants or obligations set forth in this Exhibit E may cause the County irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the County is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the County may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available to the County at law or in equity or under this Agreement.

H. Indemnification.

The Contractor shall defend, indemnify and hold harmless the County, its officers, employees, and agents, (each, a "County Indemnitee") from and against any and all infringement of intellectual property including, but not limited to infringement of copyright, trademark, and trade dress, invasion of privacy, information theft, and extortion, unauthorized Use, Disclosure, or modification of, or any loss or destruction of, or any corruption of or damage to, Personal Information, Security Breach response and remedy costs, credit monitoring

expenses, forfeitures, losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, fines, and penalties (including regulatory fines and penalties), costs or expenses of whatever kind, including attorney's fees and costs, the cost of enforcing any right to indemnification or defense under the Agreement and the cost of pursuing any insurance providers, arising out of or resulting from any third party claim or action against any County Indemnitee in relation to the Contractor's, its officers, employees, or agents, or any Authorized Employee's or Authorized Person's, performance or failure to perform under this Exhibit E or arising out of or resulting from the Contractor's failure to comply with any of its obligations under this section H. The provisions of this section H do not apply to the acts or omissions of the County. The provisions of this section H are cumulative to any other obligation of the Contractor to, defend, indemnify, or hold harmless any County Indemnity under this Agreement. The provisions of this section H shall survive the termination of this Agreement.

I. Survival.

The respective rights and obligations of the Contractor and the County as stated in this Exhibit E shall survive the termination of this Agreement.

J. No Third-Party Beneficiary.

Nothing express or implied in the provisions of in this Exhibit E is intended to confer, nor shall anything herein confer, upon any person other than the County or the Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

L. No County Warranty.

The County does not make any warranty or representation whether any Personal Information in the Contractor's (or any Authorized Person's) possession or control, or Use by the Contractor (or any Authorized Person), pursuant to the terms of this Agreement is or will be secure from unauthorized Use, or a Security Breach or Privacy Practices Compliant.

Fresno County Information Technology Standards and Preferred Practices ("IT Standards")

INTRODUCTION

Purpose

The purpose of defining standards is to ensure maximum compatibility and integration between organizations, which will provide efficient electronic interaction among parties. Maintaining standards will provide a consistent and solid framework for expanding and managing information and/or information sharing among County of Fresno departments. Maintenance of standards provides for a more stable environment by making technology easier to manage and more reliable. Resources can be leveraged more easily, thereby increasing the availability and effectiveness of technology, including application development and security processes, languages, tools, and other related technologies for the development of web enables, Internet/Intranet, on-premises, and cloud offerings.

Scope

Standards and preferred practices are developed by ISD-IT for all components of the information technology environment within the CIO's authority and control.

Standards Management

The CIO is the approving authority for granting any exceptions to these Standards and Preferred Practices.
The CIO and designee will be responsible for managing changing and emerging standards in collaboration with the respective ISD-IT disciplines and County departments.

Compliance

Compliance with Administrative Polices, Management Directives and these Standards and Preferred Practice must be maintained by all departments.

1 SECURITY

1.1 Security Organization

- **CIO** - The CIO has the highest level of responsibility for IT security for the County of Fresno.
- **County Departments** - County Departments are responsible for maintaining the integrity of the County's Security Standards.
- **Information Owner** - Usually the Department Head and/or designee of the department responsible for the information, the information owner is responsible for defining data use and management needs and charged with gathering, manipulating, and protecting the data resource to fulfill its mission.
- **IT Security Liaison** - Each County Department will have an Information Security Liaison. The Department Head may delegate responsibility for the information security function but remains accountable for security of information within the Department's control.
  The IT Security Liaison is responsible for the following:
  - A point of contact for security and management of systems that contain data and information for which the Department and/or its functions is the owner.
  - The person authorized to request access privileges and to sign security requests/changes from the Department.
  - Defining classifications of information for authorizing access and granting access privileges.
  - For advising ISD-IT of potential threats to Department information systems, including internal threats.
  - For participating in a department's self-assessment or routine security audits conducted by or under the auspices of ISD-IT.
- **County Personnel** - All County personnel (permanent and temporary employees, officials, volunteers, interns, and contractors/consultants) as individuals have a role and responsibility for protecting

information generated by or held in confidence by the County. Individuals will be held accountable for complying with County IT security policies, standards, and procedures.

1.2 Security Plan

ISD-IT will prepare an annual plan describing actions to be taken to improve information security on all major information systems. At a minimum, the Security Plan will adhere to the following standard:

- Include a statement on the status of County IT security.
- Review the prior year's security issues and remedies.
- Include identification of all scheduled audit reviews for the coming year.
- Identify any procurement needs for security equipment/software.
- Identify any changing technology standards that will impose new challenges for IT and describe how such challenges will be addressed.

1.3 Security Administration

1.3.1 Protective Measures

At a minimum, protective measures provided to protect information resources will comply with the following standards.

- Protective measures must be commensurate with a specified strength of threat.
- Deviations from normal conditions must be detected and reported timely.
- Reports of deviations from normal conditions must be responded to in a timely manner.
- Protective measures must be able to be tested to assure that they are functioning or will function to achieve, within the current County environment, the objectives for which they were implemented.

1.4 Security Awareness Program

All County staff are required to participate in cyber security awareness training prior to being given access to any County network or system. Periodically, County staff will be reminded through an on-going cyber security awareness program of their responsibility and accountability for protecting County information.

1.5 Access Control and Authorization Plan

The account and access control standards that follow apply to all County systems, applications, and data, and to all computer processing devices, including mainframe and mid-range computers, network servers, web servers, LAN servers, cloud servers, desktop workstations/computers, laptop, mobile, or handheld computers, IOT devices and to all County staff using such devices.

1.5.1 Authority for Allowing Access

Information Owners are responsible for classifying the information and defining authorized access to systems, applications, and data.

- Information Owners, in collaboration with Application Owners, are responsible for defining access levels to specific systems, applications, and data based on the principle of "least privilege," which means granting the minimum access privilege required for an individual to perform assigned job functions effectively.
- Owners may restrict the authorization of County staff and third parties to "read," "add," "update," or "delete" information on specific records or files or to execute certain computer programs.

1.5.2 Authorization

Formal mechanisms for granting authorization and access privileges must be followed by management and users (including third parties).

- Access will not be granted without appropriate authorization.

1.5.3 Role Management

User and group roles are used for user and group security management.

- Each user record contains general user information and information concerning one or more account types for a single user.
- Each group record contains all the information needed to define groups and their members. This includes the group name, the group identification number (GID), and a set of the members' login names.
- Each user and group role must have its own set of default policies and validation policies.
- For new user or group records established without specified attributes, default values will be assigned that adhere to the “least privilege” philosophy.

1.5.4 Defining Allowed Levels of Access and Authorized Activity

Official information is intended solely for the business use of the County. The County’s policy is that no individual will be authorized access to County networks, systems, or applications without a need to know based on his/her work assignment.

- Access control privilege defaults must be set to deny access when system failures occur where possible.
- System management or administrator privileges are restricted to those directly responsible for system management and/or security.
- Granting system management or administrator privileges to any County staff and/or third party requires ISD-IT, Departmental Authorized Signer approval, and business justification.

1.5.5 Security Personnel and Assignments

County staff and third parties are granted access to County information handling systems depending on the tasks the County expects them to perform.

- In keeping with these objectives, management maintains the authority to:
  - Restrict or revoke any County staff's or third party’s privileges as deemed necessary to protect County systems, data, and equipment.
  - Inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives.
  - Take any other steps deemed necessary to manage and protect County information systems.
- This authority may be exercised with or without notice to the involved individuals.
- ISD-IT is required to confirm periodically that access privileges are correct.
- ISD-IT is required to communicate any breaches of access privilege to Information and Application Owners.

1.5.6 Root\Admin Access

Root and admin access is a great responsibility, and County staff so authorized shall not abuse or misuse this privilege in any way. Root and admin access may be granted only to System Administrators.

- Root and admin access IDs and passwords may never be shared with non-authorized personnel.
- Those individuals who are authorized root or admin access are accountable for the stability and operation of networks and systems within their control.
- Any unauthorized attempts by a user or third party to gain root or admin access to any County network or system will result in disciplinary, legal, or contractual action.

1.5.7 Change Authority

- County personnel (including permanent and temporary employees, officials, interns, volunteers, and consultants/contractors) may only change production data through the authorized access privilege on applications to which they have been granted access.
- End users may not change a production system or any production system component.
- All changes to production systems must be made in accordance with the County’s Change Control standards.

1.5.8 Access Control

Access control systems must regulate access to all software and all personnel must use at least one control system to gain access. Access controls must adhere to the following requirements:

- Positive identification in the form of a County staff ID and password is required to access any network, system, application, or data within the custodial control of ISD-IT.
- Access control systems may require additional layers of security where increased protection is required.
- In all cases, County personnel (including permanent and temporary employees, officials, volunteers, interns, and consultants/contractors [including third parties directly responsible for system maintenance/administration]) are required to use any prescribed control system.

1.5.9 ID Standards

Where possible the standard characteristics for an ID are:

- County IDs must be constructed so that they can be used across County information handling systems.
- All default administrator accounts must be renamed first where possible.
- System administrators must be assigned a normal ID based on ID construction guidelines for day-to-day tasks but use a different ID based on a variation of the normal ID to administer workstations, servers, routers, or other systems.
- The standard office ID should not have administrator or PC Help Desk privileges but should be used whenever interacting with other people or external networks, such as via e-mail.
- Anonymous (or “generic”) County IDs may be used for public counter devices that must allow auto-login to authorized information only.
- Specific exceptions exist, and include:
    - Outsourced applications if the vendor has contractual authority for imposing their ID Standards.
    - Applications in which the software controls ID standards.

1.5.10 ID Management

- Everyone who receives a user ID is held responsible for all actions taken under that user ID.
- Employees are expected to exercise discretion in protecting their user IDs, i.e., the workstation must not be left unattended while logged on with a user ID. The password associated with a user ID may not be shared with anyone, even an individual with the same level of access privilege.
- IDs that have system management or administrator privileges may only be used for specific administrator tasks.

1.5.11 Password Standards

In general, the following password standards apply:

- County staff accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that County staff.
- Password must contain a minimum of 8 characters.
- Passwords must contain 3 of the following 4: upper case letter, lower case letter, number, and unique character.
- Passwords may not match any part of the display name, given name, surname, or login ID.
- Passwords may never be written down.
- Passwords should be easily remembered but hard to detect or guess.
- Passwords must be encrypted for storage or network transmission.
- The user is responsible for changing the first assigned password to one that only the user knows.
- System, software, or hardware default passwords must be replaced with unique passwords immediately upon installation.

- The display and printing of passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.
- All user-level passwords (e.g., desktop workstation, etc.) must be changed at least every 90 days.
- Password changes will be system initiated.
- Passwords that are not changed when a password change is required will be allowed to expire.
- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis or when a System Administrator leaves the team.
- All production system-level passwords must be part of the ISD-IT Security-administered global password management database.
- Users are accountable for the following individual responsibilities related to passwords:
  - Never reveal a password to ANYONE.
  - Never talk about a password in front of others.
  - Never hint at the format of a password (e.g., "my family Name").
  - If someone demands a password, report them to ISD-IT.
  - Never write passwords down and store them anywhere in your office.
  - Never store passwords in a file on ANY computer system without encryption.
  - Only use ISD-IT approved password managers to save passwords.
- If an account or password is suspected of being compromised, a report must be made immediately to ISD-IT via the service desk, and the password must be changed.
- Password history must be employed to prevent users from reusing fixed passwords. Password history must minimally contain the last ten (10) passwords for each user ID.

1.5.12 Security Administrator Responsibilities

Security Administrators are responsible for adhering to the following Standards and Preferred Practices:

- Proof of identity is required before issuing a password.
- Passwords may not be reset unless the Administrator can verify that the person making the request is authorized to access the account.
- Passwords are never disclosed.
- Administrators must reset a password, thereby requiring that an individual enter a new password.
- ISD-IT staff are authorized to refuse ANY verbal request to bypass security controls until the authority of the requestor can be verified.

1.5.13 System Administrator Responsibilities

System Administrators are responsible for adhering to the following standards and preferred practice:

- Passwords for warranty, maintenance, or other regular support activities should not expire automatically. System Administrators must closely control these accounts so that the password is not exposed to unauthorized access attempts. These accounts must have all actions logged.
- If the System Administrator determines that a system has been compromised, the individual should immediately notify ISD-IT.

1.5.14 Application Development Responsibilities

Developers of software are required to apply the following Standards and Preferred Practices:

- Passwords may not be stored in clear text or any reversible form.
- Systems must provide for role management which allows a user to take over the functions of another without having to know the other's password.
- Mask over password fields to prevent the display and printing of passwords.
- A password field that also hides the length of the password is desirable.
- Prohibit the hard coding of passwords into developed software.
- Change vendor default passwords before installing any system.

1.5.15 Session Controls

Session controls will be utilized to provide an additional layer of protection for County networks, systems, applications, and data.

- County staff must go through a log-in to gain access to County computer systems.
- Prior to initial log-in, a security notice about the system being used will be displayed.
- Accounts will be automatically locked out after a maximum of ten (10) consecutive unsuccessful log-in attempts.
- User sessions will automatically be disconnected after 20 minutes of inactivity. A logon and password are required to log back in.
- Designated systems may be required for "public" access at public counters and are, therefore, logged-in continuously, offering the public direct access to authorized public information. Such auto-logon access is designated only to specific public counter PCs and the PCs are restricted to the application serving the public.

1.5.16 Remote Access

- Access to Fresno County networks via secure remote access must be controlled using Multi-Factor Authentication.
- All remote access across a public network must be encrypted.

1.5.17 Logging and Audit Trails

Computer system logs are critical for isolating and correcting problems, but they must also support security audit functions, including detecting suspicious activities. ISD-IT is responsible for developing a Security Log Audit Plan.

1.5.18 Access Denial, Termination and Follow-up

- System and file access control permissions for all Fresno County networked systems must be set to a default that blocks unauthorized users' access.
- If a computer or network access control system is not functioning properly, it must default to denial of privileges to end-users.
- ISD-IT must perform routine reviews of logs and follow-up on excessive unsuccessful login attempts.
- Follow-up activities will adhere to incident response Standards and Preferred Practices.

1.5.19 On-going Internal Audits of Logs

Backed up and retained security logs must be for the support of internal security audits.

- The handling and review of system and security logs are restricted to authorized persons only.
- Logging must be configured to resist deactivation, modification, or deletion by any person other than the administrator.
- Retained security logs must be stored in a secure environment accessible only by designated ISD-IT security personnel.
- System and security logs must be reviewed on a regular and prompt basis.
- Logs must be reviewed whenever suspicious activity is suspected or detected.

1.5.20 Termination/Change of County Staff Access Privileges

Information and Application Owners, Managers, and County staff must periodically review authorized access privileges to consider whether changes are required.

- The individual's manager must ensure all access privileges are changed or revoked within seven (7) days of an individual's change in status.
- Requests to change County staff access privileges must be approved by the individual's Department Authorized Security Signer.
- County staff (including permanent or temporary employees, officials, volunteers, and consultants/contractors) who expect to be absent from work for a period of 30 days or more must have their privileges disabled until their return.

- Accounts that are inactive for more than 30 days will be disabled. Successful logons during any 30-day period will indicate that the account is active.
- Once County staff's access privileges have been revoked, disabled, or deleted, any transfer of information management responsibilities to another individual requires review. It also requires authorization by the Information and Application Owners prior to the establishment of access privileges to the delegated County staff member.
- All Managers must ensure that all access privileges are revoked immediately when any County staff or third-party leaves the County or is otherwise terminated.

1.5.21 Third party Access

All outside agencies requesting access to County systems must complete a contract or Third-party Agreement with the County. This contract or agreement must be approved according to established County policy.

- Agreements between the County and third parties who handle County information must include a special clause allowing the County to audit the controls used for information handling activities.
- Third-party agreements must specify the County's expectations for the protection of information by that entity.
- Third parties are subject to the same obligations and accountability for the protection of County networks, systems, applications, and data as County staff.
- Third parties that have access for the purpose of maintaining systems are subject to the County's Change Control policies, Standards and Preferred Practices.
- Third parties may not perform System Administrator duties without prior approval and authority.
- Third parties that have access to County systems will be monitored through logging and audit procedures.
- Third-party access may be revoked for non-compliance with County policies.

1.6 System Security Controls

Information systems security controls must be enforceable prior to being adopted as a part of standard operating procedure. For a control to be enforceable, it must be possible for managers to clearly determine whether:

- The control effectively performs a required security function.
- Compliance and/or enforcement of the controls can assure use by authorized personnel.

1.6.1 System Security Tools

All information security tools must be tested and accepted by the people who will work with the controls. Information security products should be selected that are easy to use, administer and audit.

- For all business application systems, security must be considered by systems designers and developers from the beginning of the systems design process through conversion to a production system.
- Whenever feasible and cost-effective, system developers must rely on system services for security functionality rather than incorporating such functionality into applications through custom code.
- To assure compliance with the County's information security standards, hardware, and software, including evaluation versions of such hardware and software, must comply with the County's Change Control Standards.

1.6.2 Database Security

To maintain the security of internal databases, access by software programs must be granted only after authentication with credentials.

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.

- Database passwords used by programs are system-level passwords as defined by the Password Policy.
- Unencrypted database credentials must not be stored in a location that can be accessed through a web server.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. If so, the following guidelines apply:
  - Database authentication may occur on behalf of a program as part of the County staff authentication process at the authentication server. In this case, there is no requirement for programmatic use of database credentials.
  - Pass through authentication must not allow access to a mission-critical database founded solely upon a remote user's authentication on the remote host.
- Access to database usernames and passwords must be restricted on a need-to-know basis. The System Administrator password is not provided too third-party.

1.6.3 Security Inspections

System administrators and security managers will periodically review computer systems to detect security standards compliance. Such inspections will also evaluate the currency of vulnerability patches and service pack upgrades.

- System administrators and security managers must install security fixes as soon as they are available and deemed suitable for installation based on the impact analysis component of the change control process.
- In no instance will a security fix be delayed for installation more than 30 days without approval of the CIO or designee.

1.7 Security Auditing

ISD-IT has the authority to perform audits or reviews of Fresno County networks, systems, or applications within the custodial responsibility of ISD-IT at any time. Authority to perform audits or reviews includes authority to audit or review third parties who have custodial or maintenance responsibility for County systems or applications.

1.7.1 Audit Frequency

Reviews must be conducted on a sufficiently frequent basis to assure that protection of sensitive information is assured. Accordingly, the following minimum frequency requirements have been established.

- Audits for critical information systems and production applications must be performed at least annually. Audits of critical systems or applications must include a risk assessment.
- Exceptions to information security policies will be permitted only by the CIO or designee.
- The exception shall document the vulnerability, the risk it poses, and suggested solution for reducing risk.
- For information classified as non-sensitive Public Records, reviews must be conducted at least every two years.
- Audits must be performed more frequently than once a year if this is necessary to conform to vendor specifications.

1.7.2 Third Party Security Audits

Security audits will include third parties with which the County has information handling agreements.

- Third parties that present an unacceptable risk must correct the risk.
- Third parties that refuse or are unable to improve their own security will have connection and access privileges denied.

1.7.3 Access to Conduct Audits

When requested for the purpose of performing an audit or review, any access needed will be provided to ISD-IT. Access includes:

- User level and/or system level access to any computing or communications device.
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted, or stored on Fresno County or third-party equipment or premises.
- Access to work areas (equipment or telecommunications rooms, offices, cubicles, storage areas, etc.).
- Access to interactively monitor and log traffic on Fresno County or third-party networks.
- All audit findings are confidential and not to be published without the consent of the CIO.

1.8 Enforcement

Enforcement action will be sought for those actions that violate Fresno County policies, Standards and Preferred Practices. Enforcement action may also be sought for those actions that fail to adhere to procedure if significant harm is caused by such failure. Any person who intentionally commits an information security violation is subject to disciplinary action which could include termination of employment, civil litigation, and even criminal prosecution.

1.9 Corrective Action

ISD-IT, in collaboration with the Information/Application owners, will establish guidelines and timeframes for correction of violations or abuses.

ISD-IT will conduct frequent reviews and perform oversight of remedial action required because of identification of abuse or violation.

2 PHYSICAL SECURITY

2.1 Facilities and Information

County departments are required to adhere to the County's facility security policies to assure the physical protection of IT Resources. Departments are responsible for controlling physical access to those information resources for which they are responsible consistent with the Information and/or Application Owner's direction.

2.1.1 Staff Offices

- Building security standards will be maintained according to Management Directive 3010.
- Persons using their cardkey to open doors are responsible for insuring that unauthorized person do not pass through while the doors are open.

2.1.2 Data Center

Entry into data center workspace areas is controlled to protect facilities, staff, equipment, supplies, and other resources against loss by fire, theft, or vandalism. Public access is not permitted into Data Centers because of the potential to change system configurations and software.

- Access to Data Center must be closely controlled.
  - Only individuals listed and approved by ISD-IT will be granted access to the County's Data Center. This list will be kept by ISD-IT and will be subject to strict enforcement.
  - Within badge-controlled areas, all individuals must wear the assigned badge so that others can verify an individual's need to be in the controlled area. Badged individuals must be vigilant for unauthorized persons and report unbadged or improperly badged personnel to ISD-IT immediately.

- Visitors or contractor personnel must always display a Temporary Security Badge. The badge must be returned to ISD-IT at the end of a visitor's authorized stay or by contractors no less than daily.
- Video monitoring, as determined appropriate by ISD-IT, will be utilized to monitor access.

2.1.3 Visitor Access

Visitor access can be granted, but the access must be for work-related reasons and must be approved by a manager who has authority for the specific work area.

- All visitors must register on a visitor log and must be escorted by the individual who is assigned to supervise and accompany the visitor.
- Visitor logs must be retained according to the County's Retention Standards.

2.1.4 Staff Status Changes

- An individual's access to limited access areas can be changed, either temporarily or permanently, without issuing a new badge or cardkey.
- Requests for access changes must be approved by ISD-IT and submitted no less than twenty-four (24) hours prior to the requested time of the change.
- Identification badges and cardkeys must be surrendered immediately upon termination of employment or contractual relationship.

2.2 Emergency Preparedness

- In each ISD-IT facility, one or more individuals must be assigned responsibility for securing high security and limited access areas against the possibility of theft of equipment or corruption or loss of data during the emergency.
- For each such assigned individual there must be an assigned back-up person responsible for double-checking facility security.
- Data Center personnel will be trained in emergency preparedness policies and procedures appropriate to their assignments.
- In no case, however, shall County personnel put themself at unreasonable personal physical risk in an imminent disaster.

2.2.1 Emergency Procedures Handbook

- Data Center operations personnel will maintain a current Emergency Procedures Handbook that will contain the following minimum information:
  - Data Center emergency evacuation procedures.
  - Data Center procedures detailing how to respond to non-evacuation emergency situations.
  - Emergency contact lists.
  - Emergency procedures testing methodologies.

2.2.2 Emergency Procedures Testing

- Emergency back-up power will be tested at least quarterly.
- Alarm system testing involving County Security, and City Fire Department must be carried out monthly.

2.3 Equipment

Protection of equipment by County departments, County personnel and third parties must adhere to the Standards and Preferred Practices detailed below.

- Upon procurement and deployment of IT equipment or devices to a County Department, ISD-IT becomes responsible for, in collaboration with the County Department:
  - Physical inventories.
  - Inventory reporting.
  - Equipment loss investigations.

- All losses of IT equipment must be reported immediately by the Department Head and/or designee having custodial responsibility to ISD-IT.
- ISD -IT is responsible for notifying the Information Owner of the loss.

2.3.1 Servers, Routers, Switches

- Datacenter servers, network and perimeter equipment must be protected from loss or corruption and must be maintained in a locked area with restricted access to only those authorized.
- ISD-IT must maintain a list of authorized access to all network equipment.

2.3.2 Desktop Workstations

Desktop workstations must be protected from theft and/or misappropriation of information.

- Public desktop workstations must be affixed to countertops and be within view of County personnel.
- It is the responsibility of County personnel to monitor the security of desktop workstations in County personnel work areas.

2.3.3 Mobile/Laptop/Handheld Devices

Mobile/laptop/handheld devices must be protected from theft. These devices must not be left alone in any setting.

2.3.4 Telecommuting with County-issued equipment

- When telecommuting with County-issued equipment of any kind the County property must be reasonably protected from theft, i.e., when left unattended, locking the exterior doors of the building.
- Locking vehicle doors or putting the equipment in the trunk of the vehicle.
- Preventing unauthorized individuals from using the equipment.

2.4 Reporting Physical Security Incidents

A physical security incident is defined as:

- Any attempt to disable, bypass, or defeat a physical security control.
- An event that management determines requires the assistance of a law enforcement agent.
- An event that results in a report of lost or missing equipment.

2.4.1 Reporting the Event

- The individual first identifying a suspected physical security violation is responsible for immediately reporting the facts of the violation to County Security, who in turn will notify ISD-IT.

2.5 Audits of Physical Security Procedures

- Annually ISD-IT will conduct an audit of physical security procedures for areas protecting County Information.
- County personnel are required to cooperate with all physical security audit efforts.

3 MANAGING IT RISK

3.1 Risk Analysis

The risk analysis process provides a mechanism for making economic decisions. To determine the nature of the risk, the information resource's sensitivity and criticality classifications will be applied to determine the type and level of protection required.

- The information resource’s value will be considered in comparison to the direct and indirect cost of protection measures.
- ISD-IT, in collaboration with Information and Application Owners will perform a risk analysis based on the risk assessment resulting from an audit, review or incident response using both qualitative and

quantitative information, including consideration of the requirements of State and federal laws and regulation and/or County policy.

- Risk analysis must be a routine component of the County's Change Control process, and results from educated knowledge about the potential impact of the change on systems, information, and users.

3.2 Mitigating Risk

If the risk is unacceptable, then protective measures must be put in place to mitigate the defined risk.

3.3 Contingency Management

It is the responsibility of ISD-IT to provide the framework for county-wide IT security contingency planning in accordance with County policy. Contingency planning includes County Department responsibility for developing Business Continuation Plans for mission critical services that are heavily or wholly dependent upon electronic information management.

3.3.1 Operational Recovery Planning

ISD-IT is responsible for developing an Operational Recovery Plan that documents steps and procedures for restoring disrupted IT services of a routine or non-routine nature for all systems and operational environments.

- Operational Recovery Plans must always be updated and current.
- For events that cause wide-spread disruption, ISD-IT will restore critical services on a priority basis.

3.3.2 Disaster Recovery Planning

ISD-IT, in collaboration with County departments, must have a mechanism for priority restoration of Information systems in the event of disaster or major disruption.

- The classifications of criticality shown below are based on an assessment of need for each information resource in terms of the duration of time that the non-availability of the resource could be tolerated without impairing the business function.
    - Immediate: Must be always continuously available to avoid causing significant impairment in the County's ability to continue core services.
    - Intermediate: Must be available within a specified period to avoid causing significant impairment in the County's ability to restore secondary services.
    - Indefinite: Could be unavailable for an indefinite duration of time without causing significant impairment in achieving the County's core or secondary business objectives.
    - Archival: This classification is assigned to information and information resources that must be retained off-line for a long period of time, usually to satisfy legal or audit requirements. Such information must be available within a reasonable period after it is requested to avoid causing significant impairment in achieving County objectives.
- The assessment of the need for availability may vary depending on the point in the processing cycle at which the non-availability of the resource occurs and will also vary with type of information.
- Accordingly, availability requirements must be established with respect to a specific period (e.g., daily, at month end or for the month before and after elections, etc.).
- To support effective Disaster Recovery Planning, County Departments will maintain an inventory of offices, work sites, and number and types of employees by site.
- To support effective Disaster Recovery Planning, ISD-IT will maintain an inventory of computer resources by site and information systems/applications in use by County Departments.
- The inventory will identify systems/applications that contain core information critical to the County's functions and government service processes.

3.3.3 Business Continuation Planning

ISD-IT is responsible for developing the business continuity planning framework to support County Departments that have mission-critical business functions significantly or wholly dependent upon viable IT resources. County Departments are individually responsible for preparing and testing such plans.

- Departments must define alternative methods, without technology support, of carrying out major business processes that cannot be interrupted in the event of a disaster or lengthy disruption.
- ISD-IT must provide the template for training in business continuity planning.
- ISD-IT will assist Departments in identification of resources to support manual functioning.
- ISD-IT will provide support for testing of the Department's plan.
- As a department implements a new automated system, it is responsible for evaluating the critical nature of the automated system.
- If there is a finding that significant reliance on an unavailable technology support tool would prevent a key business function from providing needed services in a disaster or lengthy disruption, the Department is responsible for preparing a Business Continuity Plan.

3.4 Incident Response

ISD-IT is responsible for management of an incident response that uses cross-discipline job assignees specifically trained in responding to incidents including viruses, intrusions, disasters, and cyber-crime issues.

- The primary goal in responding to incidents is to preserve the overall security of County information handling systems.
- IT related incidents will be defined in the incident response plan.
- County personnel, including employees (permanent or temporary), officials, volunteers, and consultants/contractors, whose actions contravene this standard will be subject to disciplinary action under the County's established personnel rules and procedures.
- IT related emergencies are classified Confidential until resolved. Information describing a threat, the vulnerability it exploits, its cause or its symptoms may not be distributed to anyone until ISD-IT has notified responsible parties to take corrective actions on affected computer systems.
- A threat that has been mitigated may be discussed as to cause and effect for educational purposes outside of County management channels if approved by management to do so.

3.4.1 Incident Response Team

Included within the incident response responsibility is the charge to create a cross-discipline Incident Response Team under the responsibility of ISD-IT.

- The Incident Response Team will be trained in and equipped with methodologies to monitor, prevent, detect, respond to, and recover from such events.
- The cross-discipline Incident Response Team will have access to information about potential sources of threat to the County's information systems and networks.
- To ensure a quick, effective, and orderly response to incidents, the individuals responsible for handling IT security incidents must be designated in writing, including those assigned back-up responsibilities on the Incident Response Team.
- Individuals with back-up responsibilities on the Incident Response Team will receive the same training as designees.

3.4.2 Incidents to be Reported

All incidents that relate to noncompliance with departmental policy or with County-wide or departmental information security standards, procedures or guidelines must be reported to the reporting individual's Department IT Security Designee whether it is believed the incident is intentional or unintentional.

3.4.3 Reporting Security Problems

Any end user that suspects or has knowledge of a potential or known security violation or incident is required by County policy to report the incident via the County's Incident Reporting mechanism.

- All suspected information security incidents must be reported as quickly as possible to ISD-IT.
- ISD-IT will establish procedures for prompt reporting and resolution of information security incidents.
- Any attempt to interfere with, prevent, obstruct, or dissuade staff member efforts to report a suspected IT security problem or violation is strictly prohibited and cause for disciplinary action.
- Any form of retaliation against individuals who report or investigate IT security problems or violations is also prohibited and cause for disciplinary action.
- Unauthorized disclosures of County information must be reported to the information owners by ISD-IT immediately.

3.4.4 External Reporting

- Reporting security violations, problems, or vulnerabilities to any party outside of the County (except external auditors) without the prior written approval of the CIO and/or designee is strictly prohibited.
- If required by law or regulation, management must promptly report information security violations to external authorities.
- If no such requirement exists, management will weigh the pros and cons of external disclosure before reporting problems or violations.

3.4.5 Incident Response Plan

ISD-IT will maintain an Incident Response Plan that will define:

- Incident Response Team designees and back-ups.
  - IRT Qualifications.
  - IRT Personnel Assignments.
  - IRT Training.
  - IRT Supervision and Oversight.
- Roles and Responsibilities.
- Circumstances or situations to which the Incident Response Team must respond.
- Stages of Incident Response Alerts.
- Communication Plan.
- Investigation and documentation procedures.
- Findings and Lessons Learned documentation standards.
- Contact Lists and Reporting Hierarchy.

3.5 VULNERABILITY ASSESSMENT AND TESTING

Vulnerability assessment and testing is employed for the purpose of detecting and exploiting vulnerabilities for the purpose of assessing potential risks. Periodically, ISD-IT has authority to utilize ISD-IT security staff and/or specialized members of the Incident Response Team to perform a vulnerability test.

- No advance notice is required.
- A successful penetration requires response by the Incident Response Team.
- Findings are assessed and remediation is determined on the same basis as an attack.
- Findings are applied to further improve the County's information security management efforts.

4 Personnel Security

Personnel Security standards apply to all County personnel given access to County networks, computing or peripheral devices, systems and/or applications and telephone equipment.

4.1 Responsibility

Adherence to County policies and these standards are a condition of employment or contract.

4.2 County Personnel

The following standards of responsibility will apply to all County personnel.

- Participation of all County personnel as defined above in the County's acceptable use and IT security training prior to requesting access privileges to any County networks, computing or peripheral devices, systems and/or applications, or telephone equipment.
- Access privileges are granted within the "least privilege" philosophy, based on a need to know, or assigned work expectations thereby supporting employees in demonstrating ethical work practices.
- County personnel compliance with County-wide acceptable use, IT security policies and IT Standards and Preferred Practices is a minimum standard.
- Additional departmental or contractor policies, standards, procedures, and guidelines may not conflict with County-wide IT Standards and Preferred Practices, except where departments have requested and been granted waivers and where contractors have written contractual agreements to the contrary.

4.3 No Expectation of Privacy

There is no expectation of right to privacy for County personnel and contractors that are granted access privileges to County networks, computer and peripheral devices, systems and/or applications, or telephone devices (including telephones, voice mail or fax) within the custodial control and security responsibility of ISD-IT.

4.4 IT Security as a Component of Job Assignments / Responsibilities

The following are minimum standards for incorporating IT security responsibilities within each job assignment.

- Failure to disclose material information about an individual's changed status will be treated as a violation of the County's IT security standards. Examples of such status changes include outside conflicts of interest or conviction of a job-related felony.

4.5 Reinforcing Accountability

Accountability for compliance with the County's IT security standards will be reinforced regularly through an established security awareness program.

4.6 Termination of Employment or Contract

Notification to ISD-IT must immediately follow any termination of employment or contract.

- Routine terminations in good standing must be reported to ISD-IT via REACH (ISD-IT request system) prior to close of business on the day of termination.
- Terminations in which County or contractor personnel are not in good standing must be reported to ISD-IT via ISD-IT request system as a required step in the termination process.

4.7 Penalties for Non-Compliance

It is the County's standard that appropriate penalties and remedies will be sought based on County policy and State and federal law for misuse, abuse, non-compliance, misappropriation, or theft of any information resource, including, but not limited to, equipment, data, software, intellectual property, or County or personal or financial information.

5 ASSET AND CONFIGURATION MANAGEMENT

The purpose for a formal Asset and Configuration Management function driven by standards is to assure the effective use of assets, reduce cost, increase employee and organization efficiency, and improve the County's use of the

competitive marketplace. Fresno County's approach to Asset and Configuration Management is predicated on the County's established standards for networks, hardware, and software. The County's intent in establishing these standards is to eliminate problems generally associated with rapid technological growth and change, specifically hidden costs, and preventable losses.

5.1 Inventory Management

5.1.1 Commercial Assets

- Inventory control of network, hardware, peripherals, and software must be handled via a central database.
- Procedures must be in place for updating inventories routinely as equipment and software is installed, upgraded, moved, relocated, or retired.

5.1.2 Systems and Business Applications

- All systems, business applications and databases within the custodial control of ISD-IT must be inventoried by the Asset and Configuration management Inventory Control System.
- ISD-IT will compile and annually update descriptions of major County information assets.

5.2 Configuration Management

Configuration Management provides a logical model of the infrastructure or a service by identifying, controlling, maintaining, and verifying the versions of configuration items (CI) in existence. Configuration Management provides the County a mechanism to maintain documentation of the relationship between assets. The County's Configuration Management approach will be integrated with its Asset Management program to include, at a minimum, all the following aspects:

- Planning and defining the policies and procedures and technical context for configuration management.
- Identification of the configuration structure for all infrastructure CIs, including identifiers, version numbers, labeling of each CI, and including said information into a configuration management database.
- Control mechanisms to ensure that only authorized and identifiable CIs are accepted and recorded from receipt to disposal.
- Quality controls to assure consistency and thoroughness of configurations, including changes and upgrades to any standard configuration, testing, and/or piloting.
- Performance controls to assure that changes produce the expected results and that fail back points can be efficiently and effectively achieved.
- Status accounting that provides immediate current and historical detail for each CI throughout its lifecycle, with changes to a CI traceable using the database throughout the CI's lifecycle.
- Verification and audit on an established routine to verify the physical application of the CI, and to confirm that its use is correctly recorded.

5.3 Configuration Requirements

- All equipment must comply with the following configuration standards:
  - Configuration changes must adhere to hardware and software change management standards.
  - Hardware, operating systems, services, and applications must receive pre-deployment approval by ISD-IT.
  - Operating systems must be upgraded with the most current security patch within 30 days of release.
  - Operating system configuration must be according to current established secure configuration standards.
  - All patches/hotfixes recommended by the equipment vendor and/or ISD-IT must be installed within 30 days of release.
  - Services and applications not serving business requirements must be disabled.
  - Insecure protocols as determined by ISD-IT must be replaced with more secure equivalents whenever such exist.

- Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or other similar security) or console access.
- All host content updates must occur only over secure channels.
- Security-related events must be logged and saved to approved logs.

5.4 Build and Image Management

- Builds may only be carried out by qualified and trained staff with access privileges granted to perform such functions.
- Prior to installing any build image, all new and returned from maintenance hardware must be checked for unauthorized devices, spyware, viruses, worms and/or Trojan horses.
- Prior to installing any build image, all workstations and servers must have their internal clocks synchronized to the County's standard clock.
- Software distribution and installation must be automated to the greatest extent possible.
- Images must be securely managed to assure the configuration does not become corrupted, and that when deployed the asset performs as intended.

5.5 Pre-Install/Pre-Deployment Testing

- All equipment and software must be tested prior to deployment to assure that the configuration performs according to the defined business need.

5.6 Deployment

- Changes to existing equipment and deployment of new equipment must follow change management processes/procedures.
- ISD-IT must be engaged, in accordance with hardware and software change management standards, to approve any new deployment and/or configuration change.
- Deployment of equipment and software must be thoroughly documented.

5.7 Performance Monitoring

- Accurate before-and-after performance and availability reports will be used to provide an objective measure of the impact of configuration changes.
- When negative performance impacts cannot be effectively mitigated, consideration must be given to restoring to an earlier configuration.

5.8 Usage Monitoring

- Windows-based systems will be monitored.
- The monitoring system must be capable of modification for monitoring the UNIX and mainframe environments as effectively as the Windows environment.
- The Asset and Configuration management software will use an electronic tool to automatically poll and verify user and device information.
- Usage monitoring must be used to support license management planning.
- Unused installed software must be reallocated before new software licenses are procured.
- Build standards will be periodically tested against usage information to confirm appropriateness of the build standard for a specific workgroup.

5.9 Warranty Management

- Warranty starts and end dates, supplier, and service entitlements and/or contractual agreements will be recorded and fully utilized.
- Risk and cost/benefit assessments will support decisions on roll over to post-warranty support arrangements.
- Warranty expiration alerts will advise of impending warranty end points.

5.10 Service Desk and Problem Tracking

- Problems related to performance and compatibility will be reported and tracked.
- The Configuration Management database will supply exact user specific information to the Service Desk, including any warranty and support information.
- Problems must be a critical consideration in future purchase and/or upgrade decisions.
- Problems and the cost of resolution must be considered in the Total Cost of Ownership.

5.11 Auditing

- The usage monitoring system will be used periodically to audit compliancy to County policy and these Standards.

5.12 License Management

Fresno County is committed to preventing unauthorized use of software products.

- The Asset and Configuration Management program will document and closely track all the following:
  - Licensing arrangements by vendor by contract.
  - Inventory of software licenses, including active and inactive status.
  - Compliance with licensing limitations and/or restrictions.
  - Procurement volumes.
- The Asset and Configuration Management program in coordination with ISD-IT will conduct periodic automated audits of individual servers and/or workstations to confirm compliance.

5.13 Hardware and Software Decommissioning

The Fresno County Purchasing Manager is the only individual authorized to sell, donate, or dispose of surplus County equipment.

- Retired hardware must have all hard disks "zeroized" prior to retirement to remove all software and sensitive data.
- Disposal of hardware must comply with EPA guidelines governing the disposal of hazardous waste.
- The IT Asset and Configuration Management database must be updated to reflect retired hardware and/or software.
- Proper documentation must be received for any retired hardware being assigned to any parties outside the County, including donations, sale, or disposal, to mitigate any liabilities associated with future improper disposal of such assets.

5.14 Total Cost of Ownership

The information contained within and generated by the Asset and Configuration Management program will enable the County to measure the overall cost of the IT infrastructure and to predict future IT expenditures.

- On an annual basis, the Asset and Configuration Management program will generate calculated TCO for the enterprise and for individual workstations and servers.
- IT costs must be allocated based on TCO information.

IT expenditures will be planned during budget cycles based on TCO information.

6 CHANGE CONTROL

All changes to Fresno County systems must be stringently controlled through proper planning, risk assessment, risk mitigation, planned implementation and pre- and post-change testing. All activities that will result in a change to the production environment, except defined work assignments as contained in procedure documentation, must be managed through the County's Change Control process. It is Fresno County's standard practice to utilize Change Control as a mechanism for IT managers to analyze the impact of all proposed changes to the production environment. The Change Control process creates the opportunity to coordinate the implementation of such changes through appropriate planning and scheduling to minimize the impact on end users and County productivity.

An effective Change Control program assures a:

- Single auditable mechanism for handling all changes integrated within the enterprise change control process.
- Review process for authorizing changes and involving all interested parties.
- Process for ensuring all changes are tested and validated with tested back out procedures.
- Software distribution of applications, operating systems, and packages, including source code, executable code, and parameter files, to the distributed platforms in a controlled and audited manner.

6.1 Definitions

- Production Environment - Any system or combination of equipment, systems and data used for an organization's daily work.
- Non-Production Environment - A system used only for development and testing, but not for an organization's daily work.
- Test Environment - Equipment and data, isolated from the production environment, utilized solely for testing changes or new or revised programs.
- Official Development Project - A formally defined system development effort for new and/or modified software managed through a project management plan that utilizes a change control mechanism internal to the project.

6.2 scope

The following activities must follow either the routine change control or emergency change control procedures prior to making any adds, removals, changes, or modifications to any production system.

- Addition/removal of any hardware or software to any system, including software patches, service packs and upgrades and migrations.
- Any change, meaning additions, modifications or removals of hardware, software, server(s), network, systems, applications, or configuration of hosts that reside in the production environment, including routine administrative tasks, that might affect or impact the production environment as to:
  - Availability.
  - Reliability.
  - Data integrity.
- Any change to a server, network or software that might lesson the stability of a system, and most particularly, any change that may reduce availability of an already known "unstable" system.
- Any activity that may affect or impact mission-critical systems as such systems are defined by policy or standards.
- Any change to the production system environment (air conditioning, electrical, physical moves, facility security).
- Any change to wiring or cabling, including adding, modifying, or removing such.
- Adding, modifying, or removing any established security control.

6.3 Roles and Responsibilities

6.3.1 Requestor

- Preparing and submitting the request which must contain the following minimum information:
  - Reason for the change.
  - Results expected by making the change.
  - Resources required to make the change.
  - Known impacts of the change on people and systems.
  - Known mitigation measures.
- Obtaining approval for the change.
- Preparation of the Change Control Plan.
- Testing and deployment of the plan.

- Facilitating change notification/communication.
- Change documentation.

6.3.2 Requestor's Manager or System Manager

- Expeditious handling of the request.
- Confirm legitimacy of the change request.
- Approval/disapproval of submission of the request.
- Assurance that changes control process is initiated and followed.
- Minimization of change impact on other environments.
- Ensuring efficient communication of changes.
- Ensuring changes are documented.

6.3.3 Information and/or Application Owner(s)/Analysts

- Expeditious review of the Change Request.
- Concurrence or not with the Change Request.
- Formal comment to the requestor and manager on the Change Request if no concurrence.
- Assure stability of owned environment during the change process.
- Assist with post-change testing.

6.3.4 ISD-IT Change Control Officer

- Establish and maintain updated procedures for the Change Control process.
- Facilitation of General Change Control process.
- Facilitation of Change Control meetings.
- Final approval of change request in the event of disputes.
- Maintain and publish a consolidated change schedule.
- Ensures compliance with Change Control Process.

6.3.5 Change Control Committee

- Hold regular and consistent Change Control meetings which may be electronic.
- Document proceedings.
- Establish a method for emergency change requests to be acted on non-routinely.
- Review and assess the potential technical and business impact of the change.
- Assessment of alternatives.
- Coordinate risk mitigation prior to implementation.
- Confirm that the level of resources is adequately projected and have been allocated.
- Approve/disapprove the proposed change.
- Establish the schedule based on implications of scheduling.
- Assure that the notifications include all impacted parties.
- Establish a mechanism to monitor the change effort.
- Establish a mechanism for backing out of the change if there are irresolvable problems.
- Establish a requirement for a closing report on the change.

6.4 Administrative Requirements

6.4.1 Change Control Committee Representation

The Change Control Committee will have at least one representative from each of the following areas:

- Database Administration
- Network/Radio
- Server/Storage
- Cyber Security
- Applications

- Desktop/Service desk
- Development
- ISD Customer Service

6.4.2 Frequency of Meetings

- Meeting frequency must be on an established routine, at a minimum, that assures the efficient functioning of the information management process.
- Frequency may be escalated as required for high risk or high-cost projects.
- Emergency change control requests may require unscheduled Change Control "meetings" which may be conducted electronically.

6.4.3 Record Keeping

- Discussion and decisions of the Change Control Committee on Change Control items will be recorded by the Change Control Coordinator.
- Record of Change Control proceedings will be distributed as established in Change Control procedures.
- Change control documentation (Change Control Requests, Agendas, and proceedings records) will be retained in accordance with Retention Standards.

6.5 Change Control Process

All changes to hardware, software (including application, database, and operating systems), and physical environment within any production environment must adhere to the established Change Control review and approval process. Whether the routine or emergency change control process is utilized, the process must have the following components:

- Change Control Request Format which may be electronic.
- Change Control Plan
- Review and decision-making by the Change Control Committee

6.5.1 Routine Process

- This process must be utilized for all change activities within the scope of change control that are not of an emergency nature.

6.5.2 Emergency Change Control Process

- The emergency Change Control process must be designed to be effective under emergency conditions.
- The process must be streamlined, yet thorough and complete, to encourage staff to avoid bypassing the Change Control Process.

6.6 Change Control Planning

At a minimum, Change Control planning must adhere to the following content standards:

- Stated purpose.
- Identification of potential impact(s)
- Discussion of risks and planned mitigation measures
- Implementation approach which must demonstrate:
  - Disruptions to the production and business environment will be eliminated.
  - That the change will meet scheduled implementation dates
  - That the change will not exceed projected manpower and/or system utilization
- Post-implementation/Pre-production testing
- Pilot when appropriate to the size of the change
- Training when appropriate to the size of the change
- Post-implementation evaluation

- Assignment of responsibility for documentation updates
- Closing out the Change Control effort

6.7 Expectation of Compliance with Change Control Standards

It is an expectation that all staff will comply with the County's Change Control standards. Any ISD-IT employee who fails to comply with these standards, and whose actions result in substantial lost time, downtime, or degraded performance will be subject to disciplinary action under the County's established personnel rules and procedures.

7 NETWORK INFRASTRUCTURE

The County provides all data and voice communications facilities required to perform County business based on standards contained herein. Neither County Departments that utilize the services of ISD-IT, nor individual users within such County Departments may make separate arrangements with an outside vendor to provide network or voice communication connections.

7.1 Network Infrastructure Protection

7.1.1 Energy Management

ISD-IT is responsible for assuring that an uninterruptible or alternate power source (including batteries and generator) with an appropriate level of backup power is maintained in sound condition to enable the data center personnel to implement contingencies or shut down systems safely in the event of disruption or disaster. This equipment must meet the following standards:

- Existing backup systems will be tested and improved on an established routine as follows:
  - The emergency generator will be run two times each month. Personnel are responsible for verifying that the generator starts automatically when a voltage drop is sensed. The generator will be run at each test for fifteen minutes.
  - Necessary permits to allow operation of Data Center generators during a call to reduce load before the lights go out will be secured and maintained current.
  - Centralized uninterruptible power system (UPS), emergency lighting, signage, elevator and/or security systems will be thoroughly tested on an established routine. Personnel are responsible for verifying that each continues to work for the entire expected duration of a rolling blackout.

7.1.2 Automatic Transfer Switch (ATS)

The ATS must conform to the following minimum standards:

- An alarm must indicate failure of any power source and transfer to auxiliary power.
- If there is an anomaly within the incoming power from the street, the ATS control system switches over to a battery bank. At the same time, the ATS must initiate the generator to come online.
- The system must be automatic without affecting security systems or devices being protected.

7.1.3 Battery Back-up

- Battery back-up for the Data Center must be sufficient to maintain full power for a minimum of 30 minutes.

7.1.4 Auxiliary Generator

- Generator must be fueled sufficiently to maintain 48 hours of continual operation.
- When the generator starts and becomes available, and power phasing is synchronized, the transfer switch moves input power over to the generator within 60 seconds.
- When the utility power is back on-line and stable, the input power is transferred from the generator to "street power", and the generator cycles offline. This is an automatic process.

7.1.5 Rack UPS

- Rack UPS devices must be deployed in parallel redundant configuration with N+1 redundancy to auxiliary generators.

7.1.6 Energy Testing

- The capability of the uninterruptible power source system must be tested at least quarterly, or more frequently as deemed appropriate by ISD-IT to assure normal functioning.

7.1.7 Climate Control

The County Data Center and other facilities that house significant network equipment supporting the enterprise will be equipped with appropriate climate control equipment. Climate control must meet the following standards:

- Facilities will be equipped with sensor systems to measure temperature and humidity.
- Sufficient A/C capacity to overcome the total aggregate BTUs generated by all the equipment in the data center.
- Server rooms must be static free and humidity-controlled (40% (+/- 5%)).
- Server rooms should be maintained at an optimal temperature of 75 degrees F., and must be maintained at no greater than 85 degrees F.

7.1.8 Fire Suppression

The County Data Center and other facilities that house significant network equipment serving the enterprise must be equipped with fire detection and suppression capability.

7.1.9 Inspection and Testing of New Construction

- For those Departments that utilize the services of ISD-IT, ISD-IT shall always have access to all construction sites for purposes of installing and inspecting communications facilities and equipment.
- To enable ISD-IT to inspect telecommunications facilities work, the contractor must:
  - Provide a progress schedule with the installation of telephone raceways and spaces shown as a separate item.
  - Immediately notify ISD-IT in writing of any change in architectural or mechanical drawings and specifications affecting telecommunications.
  - Provide proper access and facilities for inspections.
  - Notify the appropriate ISD-IT contact person the work is ready for inspection.
  - All systems installed by outside vendors will be required to provide a vendor inspection certificate and a vendor warranty.
- The contractor shall submit to ISD-IT a detailed test procedure. All cables shall be tested for length, attenuation, impedance, ground shorts, continuity of communications conductors and shields.
- All data cables will be tested for compliance with ISD-IT specified standards. A copy of the final test results will be delivered to the IT Manager over network in both written and electronic format. The contractor shall guarantee 100% good pairs on all cables. Failure during testing will result in re-pulling cables at the contractor's expense.
- Upon completion, copies of as built drawings related to communications work and all test results shall be submitted to the IT Manager over network for final approval and acceptance and made part of the document.
- Prior to acceptance, ISD-IT will perform an internal re-test of the contractor’s test specifications.

7.1.10 Cable Management Plan

A Cable Management Plan will be maintained as an element of the Asset and Configuration Management program. ISD-IT will maintain a written cable management plan for voice, data, and networks, including LAN, MAN and WAN and voice lines.

7.1.11 Telecommunications Rooms

Telecommunication rooms are special-purpose rooms that house telecommunications equipment. These equipment rooms have stringent requirements due to the nature, size, expense, and complexity of the equipment housed in the room. Telecommunications rooms must adhere to the Cable Management Plan standards for Telecommunications Rooms.

7.1.12 Firewalls

A firewall is a device that controls access between networks with access control lists, such as a router or similar security device approved by County standards. Firewalls establish a perimeter where access controls are enforced. All County systems playing the role of firewalls, whether they are formally called firewalls, must be managed according to the rules defined in this standard. In some instances, this will require that these systems be upgraded so that they support the minimum functionality defined in this standard. Departures from this standard will be permitted only if approved in advance and in writing by ISD-IT.

At a minimum, all firewalls must adhere to the following standards:

- Before being enabled, all new firewall services and new connectivity paths must be evaluated in terms of business advantages and security risks. Original firewall configurations and any changes thereto must be reviewed and approved by ISD-IT.
- Prior to deployment of every County firewall, a diagram of permissible paths with a justification for each must be submitted to ISD-IT. Permission to enable any paths will be granted by ISD-IT.
- All firewalls must be in locked rooms accessible only to those who must have physical access to such firewalls to perform the tasks assigned by management.
- The list of currently approved services must be documented and distributed to all systems administrators with a need-to-know by ISD-IT.
- Every network connectivity path not specifically permitted by ISD-IT must be denied by firewalls.
- Departments must not establish network connections that bypass the County firewall.
- Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to a few technically trained individuals with a business need for these same privileges.
- All firewalls must have at least two staff members who are adequately trained to make changes as circumstances require. Out-of-town vacations must be scheduled so that at least one of these firewalls administrations staff members are always readily available.
- Firewall devices must be configured and maintained only by authorized firewall administrators.
- Firewalls must be configured in accordance with least-access principles based on business need.
- All changes to firewall configuration parameters, enabled services, and permitted connectivity must be approved by the Change Control process and must be logged.
- The internal system addresses, configurations, and related system design information for County networked computer systems must be restricted such that both systems and users outside the County's internal network cannot access this information.
- Firewall filters must be documented, and current documentation must be maintained by firewall administrators.
- Firewalls must be audited on a regular basis, but no less than quarterly.
- Responsibility for managing firewalls includes responsibility for staying advised by sources providing current information about firewall vulnerabilities. Any vulnerability which appears to affect County networks and systems must promptly be brought to the attention of ISD-IT.
- ISD-IT may require additional security measures as needed.

7.1.13 DMZ

Devices that are Internet facing and outside the County firewall are considered part of the "de-militarized zone" (DMZ). These devices (network and host) are particularly vulnerable to attack from the Internet

since they reside outside the County's firewall. A DMZ is an un-trusted network connected to, but separated from the County's networks by a firewall, used for external (Internet/third party partner, etc.) access from within the County, or used to provide information to external parties.

- Production resources must not depend upon resources on the DMZ networks.
- DMZ devices must not be connected to the County's internal networks.
- DMZ equipment must be maintained in a locked rack with limited access.
- New installations must be carried out in accordance with the DMZ Equipment Deployment Process.
- Responsibility for the security of equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts.
- Contracting entities, in collaboration with DMZ support personnel and ISD-IT, are responsible for third party compliance with this standard.
- External service providers found to have violated this standard may be subject to financial penalties, up to and including termination of contract.

7.1.14 Secure Failure

If a device fails it should fail to a more secure state, with controls that are more stringent than the system that failed.

7.1.15 Modems

Use of modems is generally prohibited, and only allowed by exception when business need is clearly demonstrated in writing by the requesting Department Head. Approval by ISD-IT is contingent upon security audit of proposed modem connection with associated risk analysis.

7.1.16 Virus Protection

Virus protection is the responsibility of IDS-IT. It is the County's policy that servers, desktop, laptop, networks, network devices and mobile devices that may be authorized to connect to County networks are equipped and configured with appropriate virus protection. It is the County's policy that all systems are protected against the most common attacks. Virus protection must adhere to the following standards:

- Virus definitions are kept updated.
- All devices will be configured to use virus scanning software if available.
- All incoming and outgoing e-mail will be virus scanned.
- All e-mail attachments will be virus scanned before opening.
- All downloaded and uploaded documents will be scanned.
- New software will be scanned and confirmed virus free prior to installation.

ISD-IT is the point of contact for all incidents of significant virus threat or successful virus attack. The County's incident response standards will be adhered to in responding to successful virus attacks.

7.1.17 Intrusion Detection

It is the responsibility of ISD-IT to assure that the County's networks are protected from intrusion by unauthorized individuals by procuring and installing appropriate hardware and software. Intrusion detection must adhere to the following standards:

- Intrusion detection capability must protect County networks and data systems on a 24 x 7 basis.
- Intrusion detection must be as effective at identifying unauthorized entry from internal sources as from external sources.
- An alarm system must be utilized to alert network and systems personnel of an attempted intrusion into systems that contain sensitive information.
- Intrusion detection logs must be reviewed on an established periodic basis by ISD-IT.

The County's incident response standards will be adhered to in responding to successful intrusion attacks.

7.1.18 Third Party Connections

As ISD-IT determines that there is a business need to connect to other external business networks (i.e., Extranets), the overall network protection for County systems drops to the level of the weakest network. It is the County's policy, therefore, that only connection to trusted networks is permitted. Third party partnerships must adhere to the following standards:

- There must be a bona fide business need for the third party to have access to County of Fresno owned equipment, software, networks, or business applications.
- Requests for Third party connection must be submitted through the ISD-IT Request System.
- A Third-party Connection Agreement must be entered into between the County and the third party that addresses the terms and conditions of the agreement.
- Third party Connection Agreements that result in access to business applications that contain protected health information must meet the test for HIPAA Chain of Trust Agreements.
- The Agreement must contain a copy of the County's Trusted Partner Agreement, a Non-Disclosure Agreement, and an Equipment Sub-Custody (or Equipment Loan) Agreement if required.

7.1.19 Trusted Partners

In addition to authorized county personnel with assigned login and password access privileges, the County of Fresno does on-line business with other entities on a routine basis. These relationships require a trust relationship backed up by a Trusted Partner Agreement that defines specific security and configuration expectations. It is the County's policy that trust relationships must be defined to avoid reducing the effective protection of the County's networks.

- Trusted partner agreements must define a set of common security controls and services to which trusted partners must be bound.
- ISD-IT, in collaboration with County departments, must develop and maintain an inventory of Trusted Partners with a connection to County networks, including a description of the core business relations (i.e., the data access and/or exchanged).
- ISD-IT is responsible for establishing and monitoring Trusted Partner agreements every 5 years.

7.1.20 Non-Trusted Entities

- DMZ administrators will confine Internet or non-trusted network traffic to only one internal segment (typically containing publicly available web, FTP or TELNET) while denying all non-trusted access to the primary internal LAN.
- Servers that support non-trusted traffic will have the security configuration as generally defined in DMZ configurations.

7.1.21 Network Documentation

ISD-IT is responsible for maintaining detailed network documentation. Network documentation is considered sensitive information because it contains detailed information such as IP addresses. Diagrams that show node names are sensitive and must be protected accordingly. Network documentation must conform to the following standards:

- Internal network addresses and design data must never be released to the public; either in documentation or via the network itself.
- Network documentation must be efficiently recoverable in the event of emergency or disaster situation.

7.1.22 Vulnerability Testing

On a routine to be established by ISD-IT, ISD-IT will identify risks to the County's network. Based on the risk assessment, they will perform a vulnerability test of the IT infrastructure to exploit identified potential vulnerabilities to assure that the County's IT infrastructure cannot be penetrated by unauthorized personnel or systems.

7.2 Data and Network Services

ISD-IT is responsible for providing County-wide network connectivity between internal and external networks, including the Internet. To be connected to County networks, Department Heads must agree to comply with the County's IT Standards and Preferred Practices (SAPP), including IT security standards, to assure the highest level of service from ISD-IT.

7.2.1 Wide Area Network

The County maintains a Wide Area Network (WAN) linking County campuses throughout the County. Management of the County's WAN must conform to the following standards:

- The network must be baselined and examined for peak utilization levels, such as average and peak transition and historical views.
- Changes to network configuration or operations must be assessed for security impacts across the entire WAN, not just a segment.

7.2.2 Local Area Networks

For services to those County Departments that contract with ISD-IT as the supplier of networks and enterprise software, whether wired or wireless, the following standards will apply:

- ISD-IT will install all infrastructure wiring and network components, including running the cables from the wall plate to the users' nodes.
- A network that is expanded by non-ISD-IT personnel will be in violation of the maintenance agreement. Requests for expansion of a network will be processed by on-line submission of a request for expansion.

7.2.3 VPN

Use of VPNs will adhere to the following standards:

- ISD-IT will acquire and provide access to VPN services.
- Only ISD-IT approved VPN clients may be used.
- VPN gateways will be set up and managed by ISD-IT network administration.
- Third party users of computers that are not County-owned or configured equipment must configure their equipment to comply with the County's VPN and Network policies.
- ISD-IT will maintain an inventory of all individuals granted VPN access.

7.2.4 Wireless Networks within Buildings

In a wireless network (WLAN) wireless access points are deployed that act as transmitters sending data to wireless network cards installed on users' PCs, appliances, or mobile devices (including cell phones) anywhere on the network. Wireless networks offer the same services as a traditional wired network. Wireless networks must adhere to the following standards:

- Wireless networks will employ security mechanisms to reduce risk of interception.
- Wireless networks will adhere at a minimum to the most current IEEE 802.1X standards.
- The default SSID must be changed before an access point is put into production.
- Wireless products will be chosen for the highest level of interoperability of their security and encryption schemes.
- Wireless networks will be designed to adhere to the same security and usability standards as traditional wired networks.
- Monitoring tools will be employed in wireless applications to identify rogue access points and/or rogue users as well as alarm features to notify network administrators of network performance issues or security threats.
- All new wireless equipment must be properly hardened before deployment and must have default settings changed.
- Antennas for all wireless network devices must be positioned to limit the availability of signal outside the facility's walls.

- ISD-IT is required to conduct periodic wireless LAN audits.

7.2.5 Restrictions on Network Connections

The County provides all data and voice communications lines required to perform County business. Network connections must adhere to the following restrictive standards:

- County Departments must not make separate arrangements with a common carrier to provide network connections.
- County Departments must not establish network connections that bypass the County Firewall.
- Unless coordinated with ISD-IT, and covered by a Trusted Partner Agreement, connections that grant access to external users are prohibited.
- Sensitive information may not be downloaded at all without permission of the Information Owner.
- Employees may not use personally owned computers, peripherals, and software on a county site to perform County assigned work unless authorized by ISD-IT.

7.2.6 Wireless Device Connection to County Networks

Unsecured wireless connection to County networks is prohibited, including any wireless data communication devices capable of transmitting packet data such as personal computers, cellular phones, or other. Wireless to network implementations must meet the following secure standards:

- All wireless devices that can connect to County networks must be protected by passwords or other access control mechanism.
- Maintain a hardware address that can be registered and tracked.
- Exceptions to these standards must be approved by the CIO.

7.2.7 Routers and Switches

All routers and switches connecting to a production County network or used in a production capacity must meet the required minimum security configuration standards. Production capacity is defined as "Any network connected to the County's backbone, either directly or indirectly, which lacks an intervening firewall device; any network whose impairment would result in direct loss of functionality to County personnel or impact their ability to do work. The "production network" is the network(s) used in the daily business of the County of Fresno. Router configuration must meet the following standards:

- Router security policy must be written, approved, and distributed to all network operations personnel.
- The router IOS version must be the most recent version.
- Each router's time of day must be set accurately to correspond to ISD-IT's established clock and must be maintained with NTP.
- Unneeded network services must be disabled.
- Unused or risky interfaces and Virtual teletypes must be shut down or disabled.

7.2.8 Router Access and Configuration

- Router access and configuration responsibilities are limited to assigned trained and qualified personnel only.
- Administrators must use secure connections for router management.
- The enable password on the router must be difficult to guess and must be kept in a secure encrypted form.
- Router reconfiguration is subject to the County's Change Control processes.
- Router configuration must be well-documented with adequate administrator comments.
- Router configuration documentation must be kept off-line and must be backed up. Access to such documentation must be limited.
- It is the responsibility of the Lead Administrator to assure that on-line and off-line configuration data is synchronized.

7.2.9 Security Logging and Monitoring of Configuration Activity

A centralized means must be in place for log collection and monitoring access to domain controllers and servers which manage specifically designated sensitive information where multiple System Administrators are responsible for supporting and maintaining the infrastructure in parallel with automated monitoring and reporting tools.

- Logging must be enabled, and log recipient hosts must be identified and configured.
- All production systems that handle Confidential information must generate logs to show every addition, modification, and deletion of information.
- All system message reporting must be directed to a central logging server.
- The handling and review of system and security logs is restricted to authorized persons only.
- Logs must be set to resist deactivation, modification, or deletion by any person other than the security administrator.
- Logging must be set to include time information and must be sufficient to identify both the source and destination computers as well as the date and time each attempt occurred.
- Log files must be monitored by automation to look for and report on specific severity events.
- Communications servers must record both successful and failed login attempts.
- Proxy servers and gateways must record all failed connection attempts.
- Firewalls will record security related events based on rule sets that are defined by the firewall administrator and approved by ISD-IT. Rule sets can be defined to allow or deny access, limit function calls, and block specific addresses.
- Messages with debug severity, notice severity and higher are directed to shared user accounts that network administrators can log in and view as logging events in real-time.
- When computer crime or abuse is suspected, logs should be changed to record additional information such as the specific function called, or file accessed.
- Log files must be checked no less than weekly.
- System and security audit log files must be maintained for a period prescribed by the County's Retention Standards.
- Security audit log files that identify a potential violation that may become a personnel or criminal issue must be retained for a period prescribed by the County's Retention Standards.
- Log files must be managed to ensure the proper operation of the logging server, i.e., log files must be routinely reduced in size by archiving on a basis as documented in ISD-IT procedures.

8 SERVICE LEVEL MANAGEMENT

It is Fresno County's standard practice to utilize Service Level Management as a proactive mechanism for IT managers and responsible system administrators to review, understand and assess the significance of reduced performance and/or outages/downtime. The Service Level Management process creates the opportunity to discuss, examine root cause analysis, assess the duration and impact, and determine whether steps are in place to prevent recurrence.

An effective Service Level Management program:

- Is a critical component of daily operations management.
- Assures a high level of access to functionality for ISD-IT's customers.

A Service Level Management Plan will be maintained by ISD-IT.

9 HARDWARE

9.1 Installation and Maintenance

ISD-IT is responsible for assuring that management practices for both hardware and peripheral equipment adhere to County policy, including pre-installation inspection, maintenance, repair, and replacement.

- ISD-IT shall authorize installation of all hardware, including servers, desktop workstations, laptop computers, mobile or handheld devices.
- IT equipment must be physically and logically inspected prior to installation to check for elements that could compromise security or damage any component of the IT infrastructure.

9.2 Computer Resource Management

In addition to conformance with the ISD-IT Asset and Configuration Management program, computing resources management must adhere to the following standards:

- Procurement of hardware and software is predicated on business need and sufficiency of resources without being wasteful.
- Identification and documentation of who may and who may not install, upgrade, move, relocate, or retire IT equipment and software.
- All software installation on County hardware must comply with ISD-IT Standards and Preferred Practices
- Use of computer resources must be monitored to assure that misuse situations are readily limited, controlled, and eliminated.
- All new, upgraded, and repaired IT equipment must be physically and logically inspected prior to installation or re-installation to check for elements that could compromise security or damage IT systems or County office facilities.
- Routines must be established for on-going maintenance and refreshment of computer equipment covering each system's lifecycle.
- Procedures must be in place for maintaining documentation of equipment repairs by device, diagnostics performed, repairs, completed, and by whom and the date.

9.2.1 Servers

It is the responsibility of ISD-IT to assure effective management practices are in place for all network servers.

- Whenever possible, servers should be physically located in an access-controlled environment.
- The name, physical location and security procedures for each server must be documented.
- The County's standard security principle of least required access must be in effect for each server.
- Server ownership must be assigned and the specific responsibilities relative to each server must be documented.
- Server configuration guides must be established and maintained by each operational group for servers within the group's responsibility.
- Each server must have its secure base configuration requirements documented.
- The main functions for each server must be documented.
- System administration responsibilities must be carried out according to formal procedure.
- All servers must have logging enabled.
- The most recent security patches must be installed within 30 days of release.
- Changes in server configuration guides and changes to the base configuration of a server must be approved through the County's Change Control process.

9.2.2 Workstations

- Whenever possible, workstations will be obtained in quantities.
- A workstation manufacturer standard will be established for all workstations within the enterprise.

9.2.3 Mobile/Laptop/Handheld Equipment

ISD-IT is responsible for assuring that County departments' use of laptop computers, mobile devices is based on established business need and authorization by the County Department Head and/or designee.

- A manufacturer standard will be established for all mobile/laptop/handheld equipment within the enterprise.
- Security of such equipment must conform to the County's Standards and Preferred Practices.

9.3 Acquisition

- The acquisition of IT equipment, including hardware, software and systems must be approved by ISD-IT prior to being acquired.
- Acquired systems or hardware must adhere to the Standards and Preferred Practices and County Policy.

9.4 Equipment Replacement

- All replacement equipment will be assigned a County Asset Tag Number prior to being placed into service.

9.4.1 Servers

- Servers are to be replaced when it can be demonstrated that the server cannot efficiently run its primary application and it cannot be upgraded to provide this ability.

9.4.2 Workstations/Laptops

- Workstations/laptops are to be replaced no sooner than three years from the original date of purchase unless compelling reasons warrant replacement in less than three years.

9.5 Equipment Control

- Equipment may be repositioned within an office or cubicle to suit personal preferences, but it may not be moved from one cubicle to another or between offices or facilities without prior Department management approval and notification to ISD-IT's Asset Management office.
- Computer resources may not leave County premises unless pre-approved by both ISD-IT and the Department Head.

10 SOFTWARE, SYSTEMS AND BUSINESS APPLICATIONS

These Standards and Preferred Practices apply to all Software, Systems and Business Applications within ISD-IT's custodial authority and control.

10.1 Information Management Roles and Relationships

10.1.1 Information Ownership

For the purposes of this document, the information owner is a designated individual responsible for defining data use and management needs. Usually this is the Department Head and/or designee of the Department first charged with gathering, manipulating, and protecting the data resource to fulfill its mission.

- Information Owners are charged with the responsibility to know exactly how their organization intends to use and protect information to fulfill its mission.
- Information Owner responsibilities may never be delegated to service providers outside of the County.
- Information Owners determine appropriate sensitivity classifications as well as criticality ratings.
- Information Owners also make decisions about who will be permitted to access the data and the uses to which this information will be put.

- Information Owners must understand the uses and risks associated with the information for which they are accountable. This means that they are responsible for the consequences associated with improper disclosure, insufficient maintenance, inaccurate classification labeling, and other security related control deficiencies pertaining to the information for which they are the designated Information Owner.
- Each Information Owner must designate a "system-of-record" which will serve as the most authoritative copy of the information under his or her care. Updates to this information must be made to the system-of-record before or while updates are made to other systems containing this information.
- It is the Information Owner's responsibility to ensure that all production copies are maintained with appropriate controls to ensure a reasonable degree of information accuracy, timeliness, and integrity.
- Information Owners are further responsible for being knowledgeable about County policy and these Standards and Preferred Practices. Information Owners are accountable for assuring that systems/applications comply with these standards.

10.1.2 Application Owner

An Application Owner is the manager of the business unit or designee accountable for the functionality and performance of data resources employed in each application. Application Owners are responsible for defining requirements for how the system works, budgeting for development and implementation costs, establishing standards so that performance can be managed, and providing guidelines for collecting and distributing information.

- Application Owners must comply with the access, use and management standards established by the Information Owner.
- Application Owners are responsible for ensuring that all production copies are maintained with appropriate controls to ensure a reasonable degree of information accuracy, timeliness, and integrity.
- Application Owners are charged with responsibility for being knowledgeable about the Standards and Preferred Practices for information technology management. Application Owners are accountable for assuring that systems/applications comply with these County policies.
- Application Owner responsibilities may never be delegated to service providers outside of the County.
- Application Owners must apply a standard of "due care" to assert control practices.
- Application Owners are responsible for specifying and implementing information system controls in a manner that is consistent with generally accepted business practice and with the criticality, value, and sensitivity of the information being handled.

10.1.3 Users

User status and the level and extent of user access are determined by an Information Owner. Depending upon the level of access privilege and extent of the privilege granted to a user by the Information Owner, users may access existing information, collect, and enter new or changed information or manipulate and report on the information. The term “user" includes any County personnel (including permanent and temporary line or management employees, officials, volunteers, and consultants/contractors) provided access privileges to the County’s electronically maintained information resources. Users may also include third parties specifically designated by the Information Owner as having access privileges.

- All Users, whether County personnel or third party, are accountable by County policy for adhering to assigned access roles and for adhering to the Standards and Preferred Practices for protection of County information management assets.
- When a user’s assignment changes or County affiliation is terminated, the User’s access privileges must be immediately terminated in accordance with the Standards and Preferred Practices.

10.1.4 Information Custodians

Custodians administer the systems into which information is entered, saved, accessed, and manipulated.

- Using physical and logical access control systems, Information Custodians must protect the information in their possession from unauthorized access, alteration, destruction, or usage.
- Information Custodians are responsible for providing and administering general controls such as back-up and recovery systems consistent with the policies and standards issued by ISD-IT.
- Information Custodians are responsible for establishing, monitoring, and operating information systems in a manner consistent with policies and standards issued by ISD-IT.
- Information Custodians are forbidden from changing the production information in their possession unless they have received explicit and temporary permission from either the Owner or an authorized User.

10.1.5 Information System Developers

Information System Developers may be internal to the County of Fresno or may be an external contract provider. In either case, they are considered County personnel for purposes of the Standards and Preferred Practices. Developer's design and prepare specifications for capabilities to enter, save, access, manipulate and protect data based on the uses allowed by the Information Owner and the requirements specified by the Application Owner. The term "system developer" includes programmers, systems analysts, testers, and project managers. Developers document the configurations and the processes needed to administer each system. Once owners and custodians have agreed to functional, performance and security designs and specifications, developers build, test, train and implement the application.

- County personnel that develop systems must comply with the Standards and Preferred Practices as a condition of being hired or contracted.
- System Developers must ensure County information security standards are applied.

10.1.6 Third Parties

Third Parties are individuals or organizations who are not County personnel. Third parties may be companies that sell products or services to the County, or they may be other government or private party entities with authorization to access County information resources. Third parties may become customers or County business providers by entering into third party agreements with the County.

- Without a written and signed third party agreement, third parties are not authorized access to County information resources.
- Third party agreements contain language that limits access, use, and establishes third party responsibility for protecting County information resources.

10.1.7 ISD-IT System Managers

All production applications must have a designated ISD-IT System Manager. System managers are responsible for:

- Instituting prescribed control measures to protect information assets.
- Defining specific control procedures, implementing, and maintaining cost-effective information control measures, and performing recovery upon requests of Information and Application Owners.
- Monitor system performance and arrange for upgrades and modifications in collaboration with the Application Owner.
- Preventive maintenance programs for computer and communication systems.

10.2 Acceptable Use and User Security Requirements

Acceptable use policies are established for E-mail, Internet, Instant Messaging, and telephones.

- Users may not be granted access to County networks infrastructure or to County Systems or data prior to agreeing to comply with the County's acceptable use policy.

10.3 System Planning, Development, and Implementation

ISD-IT is responsible for assuring that standards and procedures are in place for protecting information governed by these standards, and that application development/maintenance and operational approaches are in place to support consistent compliance with the County's software and secure data management standards.

10.4 System Architecture Design

System architecture design must be approached from the perspective that the County expects systems/applications to demonstrate both high availability and high reliability. From a user's perspective, systems should be available to use at any time and provide dependable connections once put into use. Availability is the probability that a system is ready to use when called upon. Reliability (dependability) is the probability that, if available, a system will perform its designated function. Under normal working conditions it is a required standard that:

- Systems must be designed to achieve a 99 percent availability rating during normal work hours for the specific system/application.
- ISD-IT, in collaboration with the IT Steering Committee, is responsible for proactively defining and documenting the County's vision for its infrastructure direction.

10.5 System and Application Access Control

- Access to the County's IT infrastructure is restricted to authorized persons only.
- Information Owners are responsible for defining classifications of information, for authorizing access based on "need to know," defining levels of access based on roles and responsibility and granting access privileges.
- Application owners are responsible for collaborating with Information Owners to assure that system and application access control designs appropriately adhere to Information Owner use restrictions.
- ISD-IT must review and approve all new development access control designs.
- All changes to production application must be approved through established controlled release procedures established by each Application Owner, including both server and desktop platforms.
- Production users are only allowed to enter those parts of applications for which they are authorized.
- All software and hardware functions that would allow access other than that authorized will be disabled.
- Electronic file transfers to or from any County system/application are restricted to authorized individuals using an approved file transfer mechanism.

10.6 Acquisition

- The acquisition of IT equipment, including hardware, software and systems must be approved by ISD-IT prior to being acquired.
- Acquired systems or software must adhere to the Standards and Preferred Practices and County Policy.

10.7 Development

- Developers must comply with County security standards and systems conventions, including naming standards, as specified in Standards and Preferred Practices.
- Form formatted output documents must be approved by the Application Owner, the System Manager, and ISD-IT, and must identify any special handling or security considerations relative to the output.
- While undergoing development, systems and software that have disabled security controls must be partitioned from systems and software that have security controls enabled.
- Prior to pilot or production implementation, bypasses of security management tools must be removed.
- Before moving software to production, access paths that are normally not authorized to a typical production user must be removed and software should be recompiled.

10.8 System Integrity

- Systems/business applications must be developed with the means to assure system integrity, including error checking and error reporting.

10.9 System Documentation

- Complete and thorough documentation is required for production business systems, including emergency fixes and non-emergency patches.
- System design and development documentation must be completed for all new development and existing system maintenance activity whether completed internally or via an external resource.
- Releasing system documentation to third parties requires ISD-IT review to ensure County Restricted and Confidential information is not inadvertently released.
- Any modification to vendor-provided software must also be documented.

10.10 Version Control

Version control is a highly disciplined activity and must adhere to the following standards:

- New or updated versions shall be tested prior to deployment.
- Version upgrades will be assigned a new version number that corresponds to the documentation for that version. All version upgrades must adhere to all software/system documentation standards.
- Minor version modifications will be assigned a sub-number within the existing version number and must adhere to all software/system documentation standards.

10.11 Testing

- Both internally and externally provided software must be formally tested and approved for migration to the production environment prior to production use.
- When conducting system tests, access to production information must be limited to “Read-Only”.
- Security testing is required for all procurement, development, modification and/or maintenance efforts. ISD-IT, Information Owner and the Application Owner must certify that the appropriate security has been implemented.
- To assure real results during tests, developer access privileges must be reduced to that of a normal user.
- Non-production transactions used to test new software on production systems must be identified or labeled so it can be removed when testing is complete.

10.12 Acceptance

- System or software acceptance is predicated upon a demonstration through thorough testing that the system or software complies with all procurement requirements.
- User acceptance testing prior to acceptance is encouraged.

10.13 Implementation

- Before installing production systems, training & operating guides must be acquired or developed and published.
- For major or high-risk systems, a pilot implementation must be conducted and evaluated, and system remediation must be completed prior to implementation.

10.14 Operational and Procedural Documentation

- System Managers and Application Owners will ensure system and sub-system operational documentation (such as back-up and recovery) as well as procedural documentation is completed prior to release to production.
- Operational and procedural documentation will be maintained in a current state.
- Critical system operational and procedural documentation will be included as a component in each critical system’s disaster recovery plan.

10.15 Commercial Off-the-Shelf Software

- ISD-IT, with coordination from Departments using licensed software, will maintain license compliance at all times.
- Replacing of software will adhere to the standards described in these standards.
- All commercial-off-the-shelf software must include current software documentation in a form that can be made readily available to system administrators, system managers, IT Security personnel, Service Desk, and, as required, to end users.

10.16 Software Patch and Service Pack Management

The County's IT infrastructure is exposed to significant vulnerability through commercial software products.

- ISD-IT is responsible for assigning official responsibility for managing commercial software patch and service pack upgrades.
- ISD-IT is responsible for monitoring and maintaining service packs, updates, and patches.
- ISD-IT is responsible for assuming a pro-active position relative to potential software vulnerabilities and must have assigned responsibilities of routine research for vulnerabilities not widely published.
- Patches to resolve identified software vulnerabilities must be installed within a reasonable period following release by the software manufacturer at the point that stability of the patch is known.

10.17 Trial Licenses

A County Department may make special request to ISD-IT to install "trial" software provided that the software is uninstalled once the trial period has expired. "Temporarily" means that the software may be used for the terms of the license or for, at most, 90 calendar days, whichever is more restrictive.

10.18 Intellectual Property Management

10.18.1 Intellectual Property Rights

The County has legal ownership, and therefore maintains exclusive rights to patents, copyrights, inventions, or other intellectual property developed by employees, consultants, or contractors for use on County systems, except as specifically excluded by the terms of a contract. This includes intellectual property stored on County computer and network systems as well as all messages transmitted via these systems.

10.18.2 Copying and Copyrights

- County personnel may not make copies of software, data, or documentation unless:
  - It is expressly allowed by the license agreement, and
  - It is for official business.
- County personnel who make unauthorized copies of software and data may be subject to disciplinary action.
- Storing unauthorized copyrighted information and software is prohibited.
- Upon discovery, ISD-IT may remove unauthorized copyrighted information and software from County assets.
- If copyrights exist for the information posted on County websites, copyright notices must be included with the page or be readily accessible from the page before any page can be posted.
- All sources in reports and documentation must be credited. Copyright notices must also be included with in-house software & documentation.

10.18.3 Handling Third party Intellectual Property

- Unless specified otherwise by contract, all confidential or propriety information that has been entrusted to the County by a third party must be protected as sensitive information.

- It is the responsibility of each Department Head to ensure that all employees, consultants, or contractors who develop programs or documentation, or have access to County-owned intellectual property sign a Confidentiality Non-Disclosure Agreement prior to such assignment.
- County information (product specifications, databases, mailing lists, internal software, computer documentation, etc.) must only be used for the business purposes specifically allowed by the County. Use of these information resources for any other reason will be permitted only with written authorization by ISD-IT and the Information Owner.
- County software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-County party for any purposes other than County business purposes associated with specific third-party contracts or agreements.
- Exchanges of software and/or data between the County and any third party may not proceed unless a written agreement has first been signed by ISD-IT and an accountable representative for the third party. Such agreements must specify the terms of the exchange, as well as the ways in which the software and/or data will be handled and protected.
- County personnel that violate the County's policies on protection of intellectual property will have the right to access such information terminated.

10.19 Information Management

10.19.1 Information Sharing

There are significant advantages to the sharing of information between departments, including efficiency and effectiveness of the service delivery process and opportunities to improve the public's welfare.

- Information Owners are responsible for defining the rules and responsibilities for protection of shared information.

10.19.2 Database Administration

Database administrators will assure that physical design and management of County managed databases conforms to the Standards and Preferred Practices.

10.19.3 Information Classification

Information Owners are responsible for classifying information according to the standards defined below.

- Classifying information requires an assessment of the sensitivity and criticality of information resources.
- Care must be applied to avoid over-classification, which may cause unnecessary security expenditures.
- The information owner is responsible for informing Users how information may be retained, whether in electronic or physical form. This includes whether information may be printed and stored, whether individuals not afforded access to electronic records may be assigned custodial responsibility for physical forms of the same information, how electronic storage must be maintained, including retention, archive and restore.
- It is the information owner's responsibility to determine whether the classification of sensitive information resources must be properly displayed on all copies and in all forms of that resource, including on-screen displays.

10.19.3.1 Private or Confidential Data

Private or confidential data is County-held information requiring defined access and distribution controls. If released to the wrong individual, private or confidential information may have immediate or future detrimental effects. Specifically, release of private or confidential information could compromise individual privacy or expose information systems to exploitation.

- Some data collected and maintained by the County are protected from public disclosure through various privacy and confidentiality statutes, and thus, are not available under existing public information laws.
- Information Owner consent is required before granting access or releasing information.

10.19.3.2 Restricted Data

Restricted data is information that by law requires strict access and distribution control. Protection measures are prescribed by State and Federal laws and regulations which place stringent privacy and security requirements on some or all the data. Examples of restricted information include personal health information (PHI), system documentation, and details about the operating environment hosting such PHI. Information of this nature is sensitive and could have immediate detrimental effects if released to the wrong individuals.

- Access approval processes are developed for each restricted system.
- Only County personnel approved by the Information Owner are authorized access to restricted information.
- The information owner retains classification authority, access control, and distribution control responsibilities.

10.19.4 Guarding Sensitive Information

It is the responsibility of everyone granted access to sensitive information to assure that the protections and security of the information is not breached. ISD-IT is responsible for assuring that the infrastructure necessary to safeguard County information is managed and protected in a manner that maintains a consistent and reliable communication, processing, storage, and archiving environment. ISD-IT is responsible for evaluating, procuring, and configuring the protective technologies required to support the County's policy on sensitive information. ISD-IT is further responsible for working with County departments and Information and Application Owners to assure that system and electronic processes that require additional protection, such as encryption, are identified and inventoried.

- When information resources are associated with each other in such a way that access to one such resource enables access to the other associated resources, then all such resources must be assigned the highest classification of any such resources.
- Third parties must be prevented from collecting significant amounts of information.
- The original source may be retained for archive purposes if it is required by the information owner.
- Unauthorized browsing on County systems and networks is not allowed and is monitored.
- Users may not open another user's private files by violating ownership and permission restrictions.

10.19.5 Transferring Sensitive Information

- Sensitive information may not be transferred by County personnel to any individual or entity via the public internet or other insecure means.
- Sensitive information may not be transferred to any individual or entity that is not specifically authorized by law or regulation.

10.19.6 Sensitive Information on Local Devices

- County personnel must not store confidential, restricted, or protected information on any desktop, laptop, or mobile hard-disk drives unless they can first demonstrate to ISD-IT that adequate information security measures are employed consistent with the Standards and Preferred Practices.
- Information and Application Owners must approve the requested local use of sensitive information.
- Equipment with hard drives that contain sensitive information may not be reassigned, even if the sensitive information has been deleted. Prior to reassignment, hard drive media must be sanitized prior to re-use according to the County's media sanitizing standards.
- Prior to de-commissioning or destroying equipment, hard-drive media must be sanitized according to the County's media sanitizing standards.

10.19.7 Storing Sensitive Information

- All physical forms of sensitive information must be stored in a locked cabinet or desk drawer when not in use.
- Computer storage media must be classified to reflect the highest classification level of the information it contains. To avoid constantly changing data classifications:
  - Sensitive information may not be stored on County desktop computers unless security features actively protect desktop-level access.
  - Sensitive and non-sensitive information may not be co-mingled on removable storage media.
  - Sensitive information may not be stored on personal-private computers without specific authorization by the Information and Application Owner with agreement by ISD-IT.
- All information storage media containing sensitive information must be physically secured when not in use.
- Personnel who remove computer-related equipment containing sensitive information from County premises must adhere to the double protected lock standards (e.g., placing a portable computer, which contains password protected data, in the trunk of a vehicle.)
- Information and Application Owners must review the titles or other descriptions of the sensitive information for which they are responsible each year to determine whether the information is still classified appropriately.

10.19.8 Backup and Recovery

- For those systems within the custodial control of ISD-IT, backups must be carried out by qualified ISD-IT personnel on the routine established by the Information and Application Owners.
- For those systems not within the custodial control of ISD-IT, the Information and/or Application Owners are responsible for the integrity of data and are independently responsible for devising backup and recovery routines.
- Recovery methodologies must be designed based upon the critical availability requirements of the sensitive information.

10.19.9 Archiving and Retrieving

- Information and Application Owners must jointly define rules for archiving of sensitive information based on business requirements and the nature of the sensitive information.
- Archived information may only be retrieved by individuals with authorized access to the archived information based on a need to know.

10.19.10 Deleting

- Information owners are accountable for collaborating with ISD-IT in defining media sanitizing practices for deleted sensitive information.

10.19.11 Purging

- Sensitive information will only be purged from County systems based on direction from Information and Application Owners.

10.19.12 Media Sanitizing

- Media that cannot be used again (e.g., paper) must be physically disposed of according to disposal standards.
- Media that might be used again (e.g., memory cards and disks) must be overwritten, degaussed, or physically destroyed.
- Computer storage media used to store sensitive information must be “zeroized” before being sent for service or before being destroyed.
- The sanitizing of media containing sensitive information must be certified in writing.

10.19.13 Electronic Protection Measures

- Appropriate electronic protection measures must be in place for information that is defined as sensitive under federal or State law, regulation, or County policy when in active use and when stored or archived.
- ISD-IT, in collaboration with the Information Owner, is responsible for developing electronic information management methodologies that protect sensitive information.
- Such methodologies will be determined on a case-by-case basis according to business requirements.

10.19.14 E-Mail

Without positive knowledge of how mail is handled at each gateway and by each server, senders cannot guarantee that e-mail messages remain under the control of County systems.

- Sensitive information may never be mailed using group address lists.

10.19.15 File Transfer

Sensitive Information may only be transferred via secure connections as deemed secure by ISD-IT.

10.19.16 Copying and Printing

- Printing and/or copying of sensitive information is permitted only if authorization is conferred by the Information and Application Owners as required by established business process and only for the conduct of County business.
- Printed or copied sensitive information must be physically controlled but does not need to be tracked unless specifically required by an established business procedure.
- County personnel must attend equipment when printing sensitive information.
- When printing multiple-page documents containing sensitive information the User must assure that all printed pages have been retrieved from the printer.
- Waste copies and draft copies containing sensitive information must be destroyed according to County policy.
- Any third party contracted for copying, printing, formatting, or other handling of sensitive information must sign the County's confidentiality and non-disclosure agreement.

10.19.17 Disposal

- Physical material containing sensitive information (including waste material that contains Confidential or Restricted information) that is no longer required in physical form must be disposed of in a manner that assures the information cannot be accessed, reconstructed, or used for unauthorized purposes.
- The disposal of physical material containing sensitive information must be certified in writing.

10.19.18 Equipment Location and/or Relocation

- Location and relocation of equipment that contains sensitive information may not be carried out without the approval of the Information and Application Owners.
- Equipment move plans must have the approval of ISD-IT and must be accomplished by authorized ISD-IT personnel.
- Location of equipment containing sensitive information must conform to the defined privacy and confidentiality requirements of the information/application.

10.19.19 System Administration

- Security, Database and/or Network Administrators are authorized to open and inspect any user's files, including private files at the request of the Information and/or Application Owners.
- Security, Database, and/or Network Administrators who discover sensitive information stored in an inappropriate location, unlicensed applications, or other unauthorized information, must document the violation, and contact the IT Compliance Manager.
- ISD-IT will respond to the incident and assess risk to other County systems.

- Security Administrators and System Administrators may not read, use, or manipulate sensitive information not within their specific assigned and authorized information owner responsibilities.

10.19.20 Hardware Decommissioning

- Decommissioning of hardware that contains sensitive information may not be carried out until all storage media are wiped clean.
- Hardware that is to be decommissioned may not be stored pending disposal unless the storage media containing sensitive information has been cleaned.
- Formatting storage media is not an acceptable means of cleaning.

10.19.21 Administrative Protection for Sensitive Information

- Information and Application Owners are responsible, in collaboration with ISD-IT, for completing periodic information criticality and risk assessments for sensitive information for which they are accountable.
- Risk assessment outcomes define potential adjustments to information management procedures.
- ISD-IT is responsible for establishing routine internal audit procedures and assigning responsibility for managing security of sensitive information.
- County personnel who misappropriate sensitive County information may be subject to criminal penalties defined by the California Penal Code.
- In the case of protected health information, an individual who inappropriately divulges such information may be subject to financial penalties defined by the Health Insurance Portability and Accountability Act.

10.19.22 Inventory of Sensitive Information:

- All computing devices that hold sensitive information will be identified and an inventory will be maintained that describes the type of sensitive information and any specific management requirements for the specific device and the specific information.

10.19.23 Declassifying or Reclassifying Information

- Only the Information Owner can downgrade or declassify information.
- Information Owners may upgrade classifications as required.
- As information classification is upgraded the Information Owner must take immediate action to inform Application Owners, System Managers and ISD-IT of the new classification and access restrictions.
- Information Owners must conduct a periodic review to ensure sensitive information for which they are responsible has been accorded the appropriate level of protection.
- Information that is no longer deemed sensitive but still required (potentially for archival purposes) may now be reclassified as non-sensitive Public Information.

10.19.24 Encryption

Encryption standards will provide guidance to Information and Application Owners on the County's requirements for selection and implementation of encryption systems to support protection of sensitive information.

- At a minimum, the County's minimum standard for encryption will comply with the current federal security requirement for cryptographic modules, which is the federal standard for encryption of non-classified information.

10.19.25 Privacy

The County's business partners and customers have a right to expect that the personal information they share with the County to effect government services will remain private.

10.19.26 Public Information Management

Public information is information that has been declared public knowledge by someone with the authority to do so, such as the Information Owner or County Counsel, and can freely be given to anyone without any possible damage to Fresno County. Non-Sensitive public data is information that is available in the public domain, or it is County information that may be made available to the public.

- The Information Owner is the classification authority.
- Owners and managers having custody of public information have a responsibility to keep the information intact and unmodified.
- Requests for public information must be referred to County Counsel for determination of the "public" status of the information.
- Only County Counsel may decide if the information can be provided freely without any possible damage to Fresno County.

10.19.27 Information Archive and Retrieve

Archiving of data is required for long-term storage of inactive electronically maintained information.

- Archive and retrieval process details will be included within Disaster Recovery Plans for each critical system/application.