

CHAPTER 7  
INFORMATION TECHNOLOGY

<u>Section</u>	<u>Page</u>
701. General Statement.....	1
702. Definitions .....	1
703. Access Control .....	5
704. Identification and Authentication.....	6
705. User Remote Access .....	7
706. Requirements for Specific Connection Types .....	8
707. Social Media .....	8
708. Contingency Planning .....	9
709. Security Risk Assessment .....	9
710. Security Incident .....	10
711. Security Auditing and Accountability .....	12
712. Network Security .....	13
713. Wireless Security.....	14
714. Classification of Information .....	14
715. Computer Security.....	17
716. Personnel Security.....	19
717. Software and Licensing Usage.....	19
718. Physical and Environmental Security.....	20
719. Cloud Technology.....	21
720. Provision for Purchase and Internal Development .....	21
721. Acceptance of Risk and Responsibility.....	21
722. Enforcement .....	21

## CHAPTER 7

## INFORMATION TECHNOLOGY

701. General Statement. These policies and procedures adopted by the Board of Supervisors direct the delivery of technology services to departments, the use of the County's technology infrastructure by employees and the public and describes the information security practices that protect and secure Kern County's information and Information Technology (IT) resources, as required by California and federal law.

702. Definitions

.1 *Access.* Making information available to only those individuals with a business need to know – requires authorization by the Information Owner and signed Ethics and Responsible Use and Non-Disclosure Agreements.

.2 *Business Impact Analysis (BIA).* Analysis to determine the impact that certain defined disaster scenarios would have on the Department. These disasters could include short-term and long-term disasters. The intent of this BIA is to determine what processes and resources are needed in these disaster scenarios.

.3 *Business Contingency Plan.* Defines the processes needed to continue to offer business services to clients. In a disaster situation, decreased services may be required, however, this Business Contingency Plan lists how these services are to be provided.

.4 *Business Recovery Plan.* Defines the steps required to recover from a situation that had some impact on the businesses' "normal" functions.

.5 *Business Restoration Plan.* Defines the steps required to restore the business completely from a disaster that required the business to relocate, to offer limited services, or to not provide services at all.

.6 *Computer.* Devices include but not limited to desktops, laptops, thin clients, servers, and smart phones. These devices provide access to County information or resources.

.7 *Copyright.* The exclusive legal rights to publish, reproduce, copy, or sell the matter and form. If a work is copyrightable, it should be treated as if it is protected by copyright.

.8 *Distribution within.* Access within the owning Department or other County entity with a business need to know via approved electronic file transmission methods.

.9 *Distribution outside.* Access outside of the County to approved parties with a business need to know via public or private carriers and approved electronic file transmission methods.

.10 *Demilitarized Zones (DMZ's).* Area where web servers are typically located between the public and private sides of a firewall.

.11 *Entity.* Any business unit, department, group, or third party, internal or external to, responsible for maintaining assets.

.12 *Information Owner.* The Department Head and/or designee(s) assigned responsibility under state or federal law or County policy for specific data, including classification, protection and assigning access.

.13 *Information Technology Resource.* All computer, peripherals, and related equipment and software; voice communications infrastructure, peripherals, and related equipment and software; data communications infrastructure peripherals, and related equipment and software; all other associated tools, instruments, and facilities; and the services that make use of any of these technology resources.

.14 *Intellectual Property.* Documentation, software, code, copyrights, inventions or patents to which the County or a third-party has legal ownership, and therefore maintains exclusive rights.

.15 *Intrusion Detection Systems (IDS).* Application that analyses network traffic and notifies someone when suspicious activity is detected.

.16 *IT Backup and Recovery Plan.* Related to IT system back-ups and recovery. The IT Backup and Recovery Plan is provided by the relevant IT service organizations and is developed by determining the business requirements for frequency of back-ups, retention of back-up media, plans for restoring of the back-ups, and a recovery plan for restoring back-ups in an alternate IT site.

.17 *License.* Authorization by the owner of a work permitting the use of that work.

.18 *Risk Assessment Team.* County employees or contractors designated with the authority to conduct Risk Assessments.

.19 *Non-Sensitive Information.* Examples of restricted information include, but are not limited to, California Law Enforcement Telecommunication System (CLETS), Medical Examiner/Coroner, District Attorney, Public Defender and Protected Health Information (PHI), system documentation, and details about the operating environment hosting restricted information. Information of this nature is sensitive and could have immediate detrimental effects if released to the wrong individuals. Specifically, restricted information could expose individuals to danger, suspend large segments of business operations, or cause extensive damage to resources.

.20 *Private or Confidential Data.* 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. Examples of private or confidential information include:

- Passwords;
- Personal medical condition or related information;
- SSN;
- Personal or family information;
- Family names;
- Ages;
- Personal or business partner financial and banking data, including credit cards, bank routing numbers and bank account information;
- Personal identifiable information (PII) provided by constituents in the course of delivering any public health or social service (name, address, phone, SSN, family names, personal historical detail);
- County financial data not deemed public by the Public Records Act;
- Employee performance reviews, discipline reports and other personnel data;
- Information related to in progress legal proceedings;
- The combination of a logical address, User ID, and password; and
- County-owned or third-party Intellectual Property.

.21 *Protected Data.* A category of Sensitive Information. Information that may be deemed public by the Public Records Act, but if made available through public media could create vulnerabilities for the County.

.22 *Public Information.* This is information generated in the normal course of managing County operations that may be a public record under the State of California Public Records Act; however, if made available by publishing in a public medium it would create a potential physical threat or potential disruption to county operations. Examples of protected information include, but are not limited to:

- Telecommunications and cabling schematics
- Disaster Recovery Plans
- Operational Recovery Plans
- Network schematics
- Physical facility schematics
- Preliminary reorganization plans
- Detailed information about ongoing projects
- Time sensitive information
- Risk assessments
- System controls
- Evaluations of Request For Proposal's or other procurement results

.23 *Public Records.* According to California Government Code §6254.9: (a) Computer software developed by a state or local agency is not itself a public record under this chapter. The agency may sell, lease, or license the software for commercial or noncommercial use. (b) As used in this section, "computer software" includes computer mapping systems, computer programs, and computer graphics systems. (c) This section shall not be construed to create an implied warranty on the part of the State of California or any local agency for errors, omissions, or other defects in any computer software as provided pursuant to this section. (d) Nothing in this section is intended to affect the public record status of information merely because it is stored in a computer. Public records stored in a computer shall be disclosed as required by this chapter. (e) Nothing in this section is intended to limit any copyright protections.

.23 *Restricted Data.* Examples of restricted information include, but are not limited to, California Law Enforcement Telecommunication System (CLETS), Medical Examiner/Coroner, District Attorney, Public Defender and Protected Health Information (PHI), system documentation, and details about the operating environment hosting restricted information. Information of this nature is sensitive and could have immediate detrimental effects if released to the wrong individuals. Specifically, restricted information could expose individuals to danger, suspend large segments of business operations, or cause extensive damage to resources.

.24 *Risk.* Those factors that could affect confidentiality, availability, and integrity of key information assets and systems.

.25 *Policy Responsibilities.*

.25.a *Deputy Chief Information Technology Officer (Deputy CITO).* The Deputy CITO is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of Board of Supervisor.

- Ensuring security policies, procedures, and standards are in place and adhered to by entity.
- Providing basic security support for all systems and users.
- Advising owners in the identification and classification of computer resources.
- Advising systems development and application owners in the implementation of security controls for information on systems from the point of system design, through testing and implementation.
- Educating custodian and user management with comprehensive information about security controls affecting system users and application systems.
- Providing on-going employee security education.
- Performing security audits.
- Investigate reports with data/ information suspected of illegal tampering.
- Reporting to the Board of Supervisor on entity's status with regard to information security.

.25.b *General Service/ Information Technology System (ITS) Management.* The General Service ITS Manager is responsible for overseeing the technical and security implementation of a solution. Also provides oversight on all new solutions to Kern County.

- Advising systems development and application owners in the implementation of technical solutions from the point of system design, through testing and production implementation.
- Educating custodian and user management with comprehensive information about technical changes affecting system users and application systems.
- Performing reviews of all new technology changes.
- Architect and monitor the overall design, function, and effectiveness of anti-virus throughout the County.
- Report any incidents of suspected illegal tampering of data/ information.
- Review software license to conform to the Board of Supervisor's policies.
- Reporting to the Board of Supervisor on entity's status with regard to technical solutions being added or changing capability.

*.25.c County Department Head or Designee.* Kern County management who supervise users as defined below. User management is responsible for overseeing their employees' use of information.

- Reviewing and approving all requests for their employee's access authorizations.
- Initiating security change requests to keep employees' security record current with their positions and job functions.
- Promptly informing appropriate parties of employee terminations and transfers, in accordance with Kern County Policy and Administrative Procedural Manual, Chapter 1.
- Revoking physical access to terminated employees.
- Providing employees with the opportunity for training needed to properly use the computer systems.
- Promoting employee education and awareness by utilizing security policies and procedures, where appropriate.
- Initiating corrective actions when problems are identified with the Kern County information.
- Report any incidents of suspected illegal tampering of data/ information.
- Be aware of and enforce all County responsibilities pursuant to the valid software license.
- Provide all requests of firewall modifications to General Service ITS Manager.

*.25.d Information Custodian.* The custodian of the information is responsible for the processing and storage of the information. The custodian is responsible for the administration of controls as specified by the owner.

- Providing and/or recommending physical safeguards.
- Providing and/or recommending procedural safeguards.
- Administering access to information.
- Releasing information as authorized by the Information Owner and/or the Deputy CITO for use and disclosure using procedures that protect the information.
- Maintaining information security policies, procedures and standards as approved by the Board of Supervisors.
- Promoting employee education and awareness by utilizing security policies and procedures, where appropriate.
- Reporting promptly to Supervisor the loss or misuse of Kern County information.
- Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

*.25.e Information Owner.* The owner of a collection of information is usually the manager responsible for the creation of the information or the primary user of the information. This role often corresponds with the management of an organizational unit. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to the supervisor.

- Knowing the information for which he/she is responsible and created.

- Determining a data retention period for the information, relying on advice from County Council and regulations.
- Ensuring appropriate procedures are in affect to protect the integrity, confidentiality, and availability of the information used or created within the department.
- Ensure authorization of access and assigning custodianship is performed.
- Specifying requirements of securing the information to the custodian and users of the information.
- Ensure symptoms of viruses and malware are reported to the IT staff.
- Reporting promptly to the supervisor the loss or misuse of Kern County information.
- Initiating corrective actions when problems are identified with the Kern County information.
- Promoting employee education and awareness by utilizing security policies and procedures, where appropriate.

.25.f *User.* The user is any person who has been authorized to access, update, and/ or delete County information.

- Access information only in support of their authorized job responsibilities.
- Comply with Kern County Information Security Policies and Kern County IT Standards.
- Do not harm nor attempt to harm or steal any County information resources.
- Complete annual security awareness training.
- Keep personal authentication devices (ie. Passwords, PINs, etc.) Confidential.
- Reporting promptly to Supervisor the loss or misuse of Kern County information.
- Ensure County information is under control and safeguarded according to classification.

.26 *Sensitive Information.* Sensitive information can be broken down into other classifications: restricted, private or confidential, protected, and intellectual property. Sensitive information includes personal, medical records or financial information on employees, constituents, citizens, customers, business partners, or anyone else that has not been previously defined in law to be a public record. Sensitive information may also include any other information that could enable an individual to commit identity theft when so defined in law or policy. Other sensitive information includes critical infrastructure schematics or infrastructure protection plans, including buildings, vehicles, telecommunications, and systems. Information that is covered by non-disclosure agreements or intellectual property practices is considered sensitive information.

.27 *Transient Devices/Systems.* County and non-County equipment that is non-permanent including laptops, PDAs, network analysis equipment, test equipment, etc.

### 703. Access Control.

#### .1 *Access and Authorizations.*

- a. Requests for new accounts or privilege changes for County employees shall be requested by the user's supervisor and/or manager to the IT department. Employees shall be given least privilege permission to complete daily tasks.
- b. Requests for new accounts or modification to existing user/ computer accounts that are for individuals who are not Kern County employees shall be requested in writing for the department head or authorized representative sponsoring to approve. Employees who are not Kern County employees shall be given permissions on least privilege to complete daily tasks.
- c. All users shall sign a user agreement form indicating the user understands and agrees to follow all County policies, procedures, and standards. Department heads are required to ensure that the Electronic Communication Usage is provided to each employee receives a copy of the

policy and signs an acknowledgement of receipt annually. The department is to keep a file of the signed policy documented.

- d. All user accounts shall be automatically disabled after 30 days of inactivity and deleted after the Department's defined number of days of inactivity. If there are any roles that require a change to the policy the change in role will be documented and approved by the Department Head or designee.
- e. Voluntary and involuntary termination will have controlled termination provided from Human Resources of access, further guidance is in section 715.

704. Identification and Authentication.

- a. All information technology devices shall have, at minimum, a registered device or alternative contact to receive multi-factor authentication (MFA) to access the County network and password access controls to access specific systems and/or applications, including the user's unique username and passwords.
- b. Multi-factor authentication provides users access to the County network by presenting a unique password and access code. A user will be required to provide a device to register to use MFA to access the network that was not previously linked to the County. The register device will receive the notification code to enter with the username when logging into the environment. If the register device is lost or stolen, the user shall report to the Help Desk to unregister the device from the County network.
- c. Systems and/or applications connected to the County's network shall have passwords or other methods of authentication, such as token cards. Included are the minimum password requirements:
  - Passwords shall be non-trivial, at least 8 characters long.
  - At minimum the password will have upper case, lower case, special character (!,@,#,\$,%,&,\* ) and number.
  - Passwords shall be changed every 90 days.
  - Passwords shall be changed into non-identical and non-reused passwords.
- d. Each user shall positively identify themselves with authorizations that are unique to each individual user.
- e. Generic, guest or universal IDs are not permitted without a signed acceptance risk by the Department Head or designee.
- f. Group accounts, one account with more than one person with the password, are not permitted without a signed acceptance risk by the Department Head or designee. (Note: Service Accounts do not fall into this category. Service Accounts should be maintained by the administrators.)
- g. Initial authentication assigned to new users or authentication (such as passwords) changed by third-party reset shall be changed by the user at the user's next login.
- h. Users shall have different passwords for each system, application, and/ or function the user performs.
- i. All communications equipment capable of displaying system messages shall display a warning that the system being accessed is a County Information System, and that access is for official use only and is subject to monitoring. The warning has established a reasonable expectation to

limit user privacy and to be able to prosecute violators (especially under Public Law 98.473 and 99-474).

The following banner contains all the necessary elements. This shall be considered the County standard logon-warning banner.

“This system is for authorized use only. All activities may be recorded and monitored. There are no implicit or explicit rights to privacy using this system. Unauthorized or illegal use may be a felony offense punishable under Section 502 of the California Penal Code and/or other laws. Your use of this system indicates your acceptance of these terms”

For devices that have limited character length, the following banner shall be used:

“I’ve read & consent to terms in IS user agreement.”

- j. User authentication information (such as a password or a pin) shall never be disclosed or shared with anyone or left out in an openly viewable form.
- k. All users shall lock the computer or information technology device when it is not in use. The system shall also have automatic means of locking the device. The “Wait” time should be configured for ten to fifteen minutes or less. If there are situations that the device stay active, require without being interrupted the Department Head or designee will provide approval.

#### 705. User Remote Access.

Any individual or agency, hereinafter referred to as “Client”, wishing to connect to the Kern County Wide-Area Network (KCWAN) shall comply with the following list of requirements. The County reserves the right to perform periodic on-site audits of a facility to confirm that these requirements are being met. If the County determines that a Client is not meeting these requirements, at the sole discretion of County, Client will be subject to the sanctions and remedies under the law as specified in the governing Agreement, to which this is an exhibit. Violations pursuant to California Penal Code Section 502 are subject to prosecution.

.1 *Anti-virus Software.* Every workstation or server connecting to the KCWAN must have County approved anti-virus software installed on it. The anti-virus software should be configured to scan all files going to or coming from the KCWAN.

.2 *Physical Security.* All workstations, printers, network equipment, and servers connecting to the KCWAN must be physically secure. To prevent unauthorized access to the KCWAN, all users must log out of the KCWAN as soon as they have completed using the KCWAN. The County reserves the right to terminate connections after 10 minutes of idle time.

.3 *Password Security.* The Client will conform to the password standards of the county regarding application-level and network passwords.

.4 *Data Security.* Client shall have in place security procedures to ensure that all transmissions of data are authorized and to protect KCWAN data from improper access. When information must travel across lines of communication where both ends are not under the control of KCWAN, Client agrees to use, at a minimum, strong authentication and encryption to protect the data, and shall take reasonable steps to protect the data including, but not limited to, the following:

- Client will use Kern County security/access software and Kern County procedures to ensure that all transmissions of data are authorized and to protect the data from unauthorized access.
- Client will safeguard the data from tampering and unauthorized disclosures. This protection must extend beyond the initial information obtained from KCWAN to any databases or collections of data containing information derived from the data. This provision shall be in force even if data are made anonymous by removing any identifying information. Client shall



maintain the confidentiality of passwords and other codes required for accessing this information.

Client may not sell, release, or otherwise furnish such data or information to any third parties without the written approval from the Department Head or designee.

706. Requirements for Specific Connection Types.

.1 *Internet-based Connections.* If the Client is connected to an external site, outside of Kern County network the external site needs to maintain the same or higher security measures. For example, the external site should have a firewall with appropriate VPN connections. This applies to all of the following types of connections:

- Network-to-network (subnet to subnet)
- Device (e.g., PC, server, printer) to network
- Device to device
- Network to device

If the Client is an individual or agency without a network, each workstation that will be accessing KCWAN must have:

- A valid account with a reputable ISP (Internet Service Provider)
- VPN (Virtual Private Network) software installed and configured per County specifications.

If the Client will be logging into a network, the workstation must have necessary client software installed and configured per County specifications.

707. Social Media

Social Media is defined as Internet based multimedia communication, social interaction and networking. Twitter, Facebook, Instagram and Snap Chat are among a broad array of Internet based multimedia communication, social interaction and networking sites or platforms. Use of social media sites or platforms will be reviewed by County Counsel for Terms and Conditions.

1. County Departments may utilize social media to engage with the public, in an official capacity. Social media should be considered a standard and effective public information and communications practice option of the County of Kern.
2. Department Heads will be responsible for all content, including the proper maintenance, monitoring and security of that content, published by their Department using social media.
3. All content published by County Departments in an official capacity on social media may be subject to Federal and State laws concerning public records and freedom of information.
4. Department social media use will comply with all laws and policies regarding the disclosure of confidential information.
5. All passwords for social media must adhere to the minimum password requirements in section 704.
6. The following types of content are never permitted in any Department sponsored social media content, or any other official communications content:
  - Profane language or content
  - Content that promotes, fosters, or discriminates on any basis forbidden by law

- Sexual content or links to sexual content
- Comments in support or opposed to political campaigns or ballot measures
- Solicitation of commerce
- Conduct or encouragement of illegal activity
- Information that may compromise the safety or security of the public or public systems
- Content that violates any copyrighted material or infringement of intellectual property

708. Contingency Planning. To adequately address the Business Contingency Plan, each County department must have a documented plan to cover these five distinct areas:

- l. *Business Impact Analysis.* Identify critical business functions, define impact scenarios, and determine resources needed to recover from each impact.
- m. *IT Backup and Recovery Plan.* The backup and recovery plan will include the method to maintain IT data backups, storage, data restore procedures, recovery of mission critical technology, identify recover time objective, identify the frequency of backups, identify testing schedule, and applications at alternative site.
- n. *Business Contingency Plan.* Identify how business function can continue operating without interfering with normal business operation. Identify:
  - Recovery Objectives
  - Restoration Priorities
  - Roles and Responsibilities
  - Identify Minimal Deterioration State
- o. *Business Continuity Test Plan.* A plan for testing all Business Contingency Plan related activities, including, but not limited to IT data recovery and testing of contingency, recovery and restoration procedures.
  - Current copies of a department's business continuity plans shall be stored offsite at an alternate location for use during an emergency situation.
  - Testing of the plan shall be conducted periodically with an annual review of the plan.
  - As part of change control, any system, application, or network change must be reflected or considered in the Business Contingency Plan.
  - Updates and revisions to the Business Contingency Plan shall be distributed to all employees involved in the recovery process and the General Service.

709. Security Risk Assessment.

Under the jurisdiction, authority, and responsibility of the County Administrative Officer (CAO), Deputy CITO, Information Security Risk Assessments can be conducted on any entity within the County governance structure. This includes but is not limited to any information system, application, server, network, facility, and/or any process/procedure by which these systems or facilities are administered and/or maintained.

.1 *Assessment.*

- p. The Deputy CITO or Deputy CITO's designee(s) is/are responsible for the appointment of Information Security Risk Assessment Teams.

- q. Under the direction of the Deputy CITO or their designee(s), the Information Security Risk Assessment Teams have the authority to periodically conduct risk assessments to ensure the acceptable operation of the area assessed.
- r. Identify per Department and mission the applicable laws and regulations that should be included in the risk assessments requirements. Department applicable laws and regulations will also determine the frequency of security assessments being performed. A different report may also need to be prepared for unique requirements.
- s. Information Security Risk Assessments shall be conducted with the full cooperation of those responsible for the area assessed.
- t. All Information Security Risk Assessment findings shall be documented, kept confidential, and distribution limited to the necessary parties identified at commencement of the Information Security Risk Assessment.
- u. Identified vulnerabilities shall be assessed for criticality. All vulnerabilities that unnecessarily endanger or expose mission critical resources must be immediately remediated.
- v. All vulnerabilities identified for remediation shall be reported to and acknowledged along with the Department's response to the Deputy CITO or Deputy CITO's designee(s).

*.2 Security Exception.*

- a. Requests for exceptions should contain the following information:
  - Identification of the policy for which the exception is being requested.
  - A description of how the exception is contrary to the established policy.
  - A description of the justification for the exception.
  - A description of the benefits the County would gain by granting the exception.
  - Identification of the risks associated with the granting of the exception.
  - A description of the steps that will be taken to mitigate any potential security risks to the County.
  - Provide any additional information requested by the Security Exception Review Committee.
- b. Deviations from Information Security policies and standards shall not be permitted without written approval via an authorized exception review process conducted by a Technical Advisory Committee (TAC) appointed Security Exception Review Committee.
- c. Evaluations of exception requests will take into account the compensating benefits to the County in each exception request. Requests that create significant risks without compensating controls will not be approved.

710. Security Incident.

*.1 Security Incident Types.*

- a. Actions intended to harm or illegally access County information resources or information.
- b. Potential violations of Federal law, State law, and/ or County Policy involving a County information technology resource or information.

- c. A breach, unauthorized access of a County information technology resource or information. The incident may originate from the County network or outside the network.
- d. The infection of any County system with a digital virus including but not limited to: worm, Trojan horse, rootkit, bot, virus, or other type of malware.
- e. Action or attempt to utilize, alter, conduct a denial of service, or degrade a County owned information technology resource in a manner inconsistent with County Policies.
- f. The unauthorized use of an information technology resource or information.
- g. Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

#### *.2 Security Incident Response Team.*

- a. Notify the Department's designated Information Security Representative (ISR) or IT Supervisor/ Manager immediately of any suspected or real information security incident.
- b. The ISR will form an Incident Response Team. The Incident Response Team shall be made up of individuals from many technology disciplines, and trained on the process of how to respond to a security incident. The ISR and Incident Response Team will coordinate an investigation and/ or corrective action plan deemed necessary in response to the information security situation.
- c. Reports shall be generated from the incident and kept by the department to maintain records. The reports shall be given to the Deputy CITO and Department head for review and compile of statistical analysis.

#### *.3 Incident Reporting.*

- a. Employees shall promptly notify their IT staff or if there is no local staff assigned notify the General ITS staff for the following:
  - Intrusion attempts, security breaches, theft or loss of County information and other security related incidents against the County.
  - There is knowledge or a reasonable suspicion of an incident which violates the confidentiality, integrity, or availability of County information.
  - A virus, worm, bot, rootkit, or other malware has been discovered.

Incident Reports shall include:

- A description of the event
- Approximate timelines
- Parties involved and report status
- Resolution of the incident (if any)
- External notifications made (if required)

#### *.4 Incident Escalation.*

- a. Upon notification of an incident the Information Technology Manager or designee, as needed, shall escalate to the Incident Response Team.
- b. If activated, the County's Security Incident Response Team shall plan and coordinate the activities with the Department Head and other departments if applicable. During the

identification of the incident until the incident is considered resolved the following decisions include, but are not limited to:

- Restricting information system access or operations to protect against further information disclosure.
  - Involving law enforcement agencies in cases where applicable statutes appear to have been violated.
- c. All external notification, reporting or publicizing shall be approved by the Department Head or the designee.

*.5 Incident Actions.*

- a. If the incident appears to involve a compromised computer system, the state of the computer system shall not be altered and the system should be immediately pulled from the network.
- b. Whenever system security has been compromised or if there is a convincing reason to believe that it has been compromised:
- All passwords residing on the system or account compromised shall immediately be changed.
  - Compromised system should reload the operating system and all applicable software to a known trusted state.
  - All changes to user privileges or access to unauthorized resources during the time of the suspected system compromise shall be immediately reviewed by the systems administrator for unauthorized modifications.

711. Security Auditing and Accountability.

*.1 Incident Requirements.*

- a. All information technology resources throughout the County shall be regularly accessible and auditable. Audits may include, but not limited to:
- Ensure integrity, confidentiality, and availability of information and information technology resources.
  - Monitor users or systems activity where appropriate.
  - Verify that vulnerability management is being maintained at the appropriate security level.
  - Verify that antivirus and other system protections are being maintained at current levels.
  - Validate compliance with stated security policies.

*.2 Logging.*

- a. Users shall be notified through the County's Appropriate Use Policy of expected activities allowed on information technology resources and all actions taken on information technology resources are logged. At any time the logs can be reviewed for violations to County Policies.
- b. County computer and communications systems shall securely log all significant security events. Security events include but are not limited to:
- Account logon events
  - Account management
  - Password guessing attempts
  - Changes to user privileges

- Electronic configuration policy changes
- Attempts to use unauthorized privileges
- Attempts to access unauthorized objects
- Changes to logging subsystems

712. Network Security.

*.1 Network Security Description.*

- a. The Security Perimeter is defined as all resources, systems, connectivity, and services responsible for enabling and maintaining connectivity between the County, its business partner(s), and all other external-to-organization resource(s) or service(s). It represents the “managed point of entry/exit” to County infrastructure resources. It includes but is not limited to Firewalls, Intrusion Detection Systems (IDS), Demilitarized Zones (DMZ’s), remote connectivity resources, and the network architecture resources providing connectivity for the environment.
- b. The General Service Information Technology Services Division (ITS) is responsible for the Security Perimeter and its management. Departments must submit to General Service ITS for approval, any plans that may require modifications to the Security Perimeter or any changes that could affect the Security Perimeter. General Service ITS will assure that any changes, additions, or deletions from the Security Perimeter adhere to current Information Security Perimeter Standards as adopted by Kern County.
- c. General Service ITS may take any action deemed necessary to ensure the security of Kern County resources. This includes but is not limited to:
  - Termination/Shutdown of connectivity
  - Termination/Shutdown of services
  - Termination/Shutdown of resources
  - Termination/Shutdown of systems

*.2 Network Security Requirements.*

- a. Perimeter devices where capable and appropriate, shall be configured in such a manner as to not divulge their function and/ or location.
- b. All devices, including perimeter devices, shall display warning banners for logons.
- c. Perimeter devices shall have unique passwords and/ or access methods or the use of Terminal Access Controller Access Control System (TACACS) and/ or Remote Authentication Dial-In User Service (RADIUS).
- d. Perimeter components shall be secured through physical and logical security measures allowing only authorized administrator access.
- e. Perimeter devices shall provide for auditing and logging.
- f. Router(s) and Switch (es), where appropriate, shall be configured with Access Control Lists (ACLs) that limit administrative access and have a Deny All statement at the end of the list.
- g. Unused ports shall remain in an inactive or shut status until required to be activated for connectivity.
- h. All connections shall be clearly labeled and identified.

- i. All circuits shall terminate on a County Router in the General Service ITS department where possible.

713. Wireless Security. This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of the County internal networks. This section prohibits access to County networks by unsecured and unauthorized wireless communication mechanisms. This includes any form of wireless communication device capable of transmitting packet data. To comply with this policy, wireless implementations must:

- a. Have the design reviewed and approved by General Service ITS.
- b. Must comply with current County Wireless Security Standards and Procedures.
- c. Must have the final installation approved and tested by General Service ITS before the wireless network goes into production.
- d. General Service ITS has the authority to shut down wireless solutions that have not been tested or approved by General Service ITS.

714. Classification of Information.

*.1 Classification of County Information.*

- a. All information is categorized into two main classifications:
  - Public
  - Sensitive
- b. Public information is defined by the California Public Records Act, and is contained within California Government Code 6254.9.
- c. Sensitive information is any information declared by law or policy to be non-public information. Sensitive information includes the following:
  - Restricted Data
  - Private or Confidential Data
  - Protected Data
  - Intellectual Property
- d. The Information Owner is the classification authority. It is the responsibility of the Information Custodian to apply appropriate measures to protect electronically processed and stored information so classified by the owner of that information.
- e. Only County personnel designated in writing and approved by the information owner are authorized access to restricted information. Access approval processes are developed for each restricted system. The information owner retains classification authority, access control, and distribution control responsibilities. The owner Department designates restricted data and systems in writing to the Information Custodian. Restricted data may also be contained in the following elements of restricted systems:
  - Computer readable files
  - Reports and Printouts
  - Terminal and Monitor displays
  - Program Source and Object code
  - Systems and Program documentation
  - User documentation

- Information related to in progress legal proceedings
  - The combination of a logical address, User ID, and password
  - County-owned or third-party Intellectual Property
- f. Only County personnel with a designated need-to-know, or others with Board approval and within any overriding state or federal statute or regulation, are authorized access to private or confidential information. The information owner retains classification authority and only the information owner is authorized to approve or disapprove both access and distribution requests. All requests of any nature to release Private or Confidential data to an entity outside of the County, whether a private request or an order of a Court, must be reviewed and approved by County Counsel and the CAO prior to release. County Counsel and the CAO will also determine if any form of protection, such as a Non-disclosure agreement, is required to protect the data from further unauthorized release.
- g. Work products that are in a draft or preliminary form are not subject to the Public Records Act referenced above and should not be released outside the County without specific approval of County Counsel and the CAO. Work products, such as those listed above, that are in final form should only be routinely accessed by County personnel whose job function requires access for normal business purposes. The information owner retains classification authority and provides general guidelines regarding release of the information outside the County. County managers are authorized, based on those guidelines, to approve or disapprove both access to and distribution of requested information. When in doubt however, managers must always obtain Department information owner consent before granting access or releasing protected information. It is strongly recommended that the CAO and County Counsel be consulted and a Non-disclosure agreement be executed by the requesting entity if it is felt to be in the best interests of the County to restrict further distribution of the information.
- h. *Intellectual Property.* Without specific written exceptions, all programs and documentation generated by, or provided by employees, consultants, or contractors for the benefit of the County are the property of the County. 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. This includes intellectual property stored on County computer and network systems as well as all messages transmitted via these systems. 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.
- i. Registered software purchased from a non-County source is considered third-party intellectual property. Ownership and limitations on use are established by the registered owners' licensing agreements.

## .2 *Information Classification.*

- a. Information ownership is the direct responsibility of user departments. Department Heads and/or designee(s) are responsible for being knowledgeable about confidentiality and privacy laws specific to their department's functions. Department Heads and/or designee(s) are responsible for all aspects of the classification, use, distribution and protection of County information within and outside of their respective departments. This responsibility includes determining the level of access to be granted to a user. Information owners are responsible for coordinating with the Information Custodian to assure that facility security needs of sensitive information are met.
- b. Information that has been identified as sensitive shall be protected by a nondisclosure agreement or other appropriate document with outside professional services contract.



### *.3 Storage and Media Control.*

- a. Sensitive and restricted information shall be kept from view of unauthorized people. Access to work areas containing sensitive and restricted information shall be physically restricted. Visitor access to work areas shall be controlled by guards, receptionists, or other staff.
- b. Printers that are printing sensitive and restricted information shall not be left unattended until the printouts are removed or destroyed.
- c. All sensitive information stored on media (such as hard disk drives, USB sticks, magnetic tapes, CD-ROMs, etc.) shall be encrypted and physically secured when not in use. Sensitive and restricted information transferred to laptops, PDA's and all other portable media shall be encrypted. These laptops, PDA's and all other portable media shall remain in the possession of the traveler at all times.
- d. Any medium for backup/ recovery shall have the same or better access and security controls as the original information.
- e. Sensitive and restricted information shall not be stored any longer than the business function or law requires.
- f. Equipment that is no longer under the physical control of the County shall have protected information purged/ cleared prior to transferring control to an outside agency (e.g. surplus, sending equipment out for repair, loaning equipment, etc.). Alternatively, repair vendors shall execute a nondisclosure agreement with the County.

### *.4 Disposal.*

- a. Electronic information shall be purged/ cleared or zeroed if the device stored sensitive information.
- b. Media shall be reliably electronically erased and/ or physically destroyed. Some departments may have disposal services in place and will dispose of media through the designated bins.
- c. Departments that have surplus equipment shall appropriately purge and/or destroy the data stored on the device. Equipment that will be discarded and not reused shall be shredded or destroyed until the equipment is not readable. Equipment (such as but not limited to hard drives or memory based devices) that will be reused by another department or sold outside of the county to recover cost of the device will be cleaned by overwrite technology. For specific guidance on the number of times the media should be wiped refer to NIST 800-88 Special Publications.
  - The department will identify if the equipment is still usable or not. If the equipment is usable refer to Chapter 5 on the surplus property disposal. Equipment valued \$1000 and over are entered into the Inventory Adjustment Request (IAR). The IAR will have a field that shall be completed by the IT manager and approved by the Department Head or designee to ensure the equipment was cleaned during the disposal process. Equipment identified as unusable and able to store sensitive data valued under \$1000 will be tracked in the Capital Asset database under the Unusable Disposal Adjustment form (UDA). The UDA will track the equipment being cleaned and disposed. The Department Head or designee will provide annual approval of the equipment being cleaned and entered into Capital Assets. The Purchasing, Auditor, and Deputy CITO departments will have the ability to view the UDA.

### *.5 Declassifying or Reclassifying Information.*

- a. Only the Information Owner may downgrade or declassify information. Downgrading is the process, as an example, of reclassifying information from “Restricted” to “Confidential.” Declassifying is the process of reclassifying information from “Confidential” to “unclassified” or “Public.” Specific procedures may exist for specific categories of Private or Protected information as mandated by other state or federal regulations.

.6 *Encryption.*

- a. Encryption keys used for County information are sensitive and restricted as protected information. Encryption keys should not be shared with vendors, contractors, or third parties without written approval from the Deputy CITO or County Counsel. Encryption keys should always be transmitted over an encrypted network link.
- b. Whenever possible the County shall employ automated key management for the protection of County information on the network.

Refer to the Information Technology Standards for encryption specifics and standards.

715. Computer Security.

.1 *General Security.*

- a. All information technology devices shall be as fully protected as possible from malware and unauthorized changes. Example of malware, include computer viruses, worms, Trojan horses, rootkits, bots, and other unwanted software.
- b. All software running on County devices shall utilize the latest security updates provided by the software vendor or as addressed in County standards.
- c. All information technology devices that can accept antivirus software shall run the latest signature from vendor on the device. If there are identified devices that cannot operate with antivirus software, document and get approval from the Department Head or delegated designee.
- d. All users shall exercise caution when accessing files from the internet. Files should only be accessed from reputable sites.

.2 *Email Security.*

- a. County information technology resources, including e-mail, shall be used for County business purposes. Policies for incidental and non-business use of County information technology resources must be defined by each individual County department.
- b. Access to e-mail services is a privilege that may be wholly or partially restricted without prior notice or without consent of the user.
- c. Kern County government retains all property rights in any matter created, received or sent via the County’s information technology systems and such matter is not the property of the employees. Employees should have no expectation of privacy in any matter created, received or sent using the County’s information technology systems.
- d. All users shall exercise caution when opening email attachments. Only open attachments from expected recipients.
- e. All e-mail is subject to audit and periodic unannounced review by authorized individuals as directed by the Director of each department, without the permission of the sender or recipient.

The County reserves the right to override any individual password and access all electronic mail messages for any purpose, and to disclose such matter to authorized individuals within the organization.

- f. Email attachments and downloaded files shall be scanned for viruses and isolated if a virus is detected.
- g. E-mail is subject to the policies concerning other forms of communication as well as all other applicable policies including, but not limited to, confidentiality, conflict of interest, general conduct and sexual harassment.
- h. E-mail services shall not be used for purposes that could reasonably be expected to cause directly or indirectly excessive strain on the e-mail system or unwarranted or unsolicited interference with others' use of e-mail or the e-mail system.
- i. County departments shall take appropriate steps to protect all e-mail servers from various types of security threats as follows:
  - Place e-mail servers in safe locations that are physically secured.
  - Back-up the e-mail servers for software and data on a regular basis.
  - Run anti-virus software on the e-mail servers to protect the server itself. Apply the same security guidelines to the e-mail servers as to the other County servers.
- j. Employees shall only access e-mail through systems set up by the County. Employees shall not access Hotmail, AOL, Yahoo, Google, and similar e-mail accounts over the County's Wide Area Network (WAN) including web-based e-mail hosted outside the County. It has been detected that these types of e-mail accounts bypass the County's security network and make the County's WAN vulnerable to viruses.
- k. E-mail generates correspondence, which may be recognized as official records in need of protection/retention in accordance with the California Public Records Act. Therefore, electronically stored mail is subject to retention requirements. Sensitive email shall be stored to another location to retain the information. The location shall be secured to the requirements of the policy. Retention of e-mail should be kept to the minimum required by law and business purposes.
- l. Encryption of e-mail may be appropriate in some instances to secure the contents of an e-mail message. Each user should be cognizant of the sensitivity of information contained in e-mail and understand that it may be passed beyond the intended recipient. Encryption must follow County Information Technology Standards.
- m. Occasionally there is an immediate need to transmit confidential information. The use of e-mail is often the most expedient process, but also poses a considerably higher risk of breach of confidentiality. As with paper records, important safeguards must be in place to protect the information contained in e-mail so that it reaches its intended destination in a secure manner. Additional safeguards (such as the use of password protected attachments and/or the use of encryption techniques) should be employed when dealing with sensitive or confidential information.

### *.3 System Maintenance.*

- a. Maintenance activities shall be approved by the IT supervisor or manager.
- b. Vendors and/ or contractors that perform maintenance on County devices shall be authorized and monitored.

- c. Vendors and contractors needed to perform the maintenance in a County building will be escorted and monitored.

716. Personnel Security.

*.1 Voluntary Separation/ Termination.*

- a. Removal of access privileges, computer accounts, and authentication tokens shall be performed the day after the personnel leave employment.
- b. Personnel shall return any keys and/ or property to a supervisor or manager.
- c. Supervisor or manager shall inform annually in writing an individual of his/her responsibility to abide by the non-disclosure agreement and privacy of County information.
- d. Verify files and information under the user's control are available or transferred to the department.

*.2 Involuntary Termination.*

- a. Terminating access immediately, preferably at the same time (or just before) the employee is notified of dismissal. Termination can include layoffs or termination of cause.
- b. If access is needed to complete job duties the permission should be limited to minimal permissions.

*.3 Termination Process.*

- a. The IT department shall be notified by Manager, Supervisor, and/ or Human Resource Department in advance of an employee's termination and IT shall be provided a list of all permissions granted.
- b. Ensure the individual's account(s), including standalone applications, have been disabled.
- c. Ensure the individual's name has been removed from any internal system access list, firewall lists, etc.
- d. Terminate remote access account(s) and access tokens (if applicable).
- e. Assign files and directories access rights to the individual taking the departing personnel's responsibilities (if applicable).
- f. Re-route email to the appropriate person identified by department management (if applicable).

*.4 Department Transfers.* Personnel that are transferred to another department within the County shall have access to County information reviewed for appropriate access needed. The supervisor or manager can confirm required access needed. All other access should be taken away when not needed.

717. Software and Licensing Usage.

*.1 Use only legally acquired and licensed software.*

- a. A software license is a license to use the software by a specific device or by a specific number of users. A software license does not give ownership of the software to the Licensee and generally restricts the user's rights to a few very specific uses.

- b. There is a significant financial liability to the County if software that has not been legally obtained is used on County-owned or leased equipment.
- c. Only software that has been legally acquired and licensed by the County for County use may be used on County owned equipment. A department head or designee may make exceptions for a period of 30 days or less for evaluation purposes, after having determined that such use of third party software is legally allowed under the license for that software and after having determined the software is virus free.
- d. Only software that is specifically licensed for Home Use may be used on personally owned computers of employees.
- e. Copies of software must not be made for use on secondary computers, such as County owned laptops, unless the software license specifically allows for such copies to be made and used during periods of non-use on the primary computer.
- f. Generally you may only make copies of software for back-up purposes.
- g. Only the Board of Supervisors or the County Purchasing Agent has the authority to accept the terms and conditions of a software license. This authority may be delegated by the Board with certain restrictions and established procedures to be followed.
- h. Department Heads or designee are authorized by the Board of Supervisors to click "I Agree" to download and purchase software and software maintenance through the Internet, on their own authority. For further information on the "I Agree" software agreement refer to the "I Agree" Software policy.

*.2 County Developed Software.* Software developed at the expense of the County, either by County staff or contractors, inclusive of derivative works, is considered intellectual property owned by the County. The Department is responsible to the originating funding source for reasonable and proper use/disposition of the intellectual property just as it is with physical property. Any release of County owned intellectual property to other entities, public or private, must be based on sound business practices. However, software that has been developed with funding from the state or federal government may likely be considered public domain to the extent it might have to be made available to other government entities free of charge except for the cost of duplication.

718. Physical and Environmental Security.

- a. Review and retain logs of system level security violations and retain records per the statutory requirements.
- b. Identify and enforce physical security requirements including controlled access.
- c. Records shall be maintained of individuals assigned access codes/keys/combinations, limiting distribution of computer center or information facility access codes or keys (e.g., hard, proximity, magnetic stripe) and combinations only to those employees needing entry to fulfill their job requirements. Records shall be maintained and kept current, an inventory of physical computer and information resources including peripherals.
- d. Records shall be maintained and kept current of a list of authorized service vendors entering the computer center for repair and maintenance of equipment.
- e. Report the loss or theft of an information resource to management and complete required forms, if any, and complete a written incident report to be kept with departmental inventory. If appropriate, notify the Auditor's office of the loss or theft as required.

- f. Notice suspicious individuals (e.g., maintenance, public and others visiting the organization, delivery personnel, vendors, etc.) and be prepared to challenge individuals entering the computer center or other restricted areas.

719. Cloud Technology.

- a. Cloud communications services provide a shared pool of configuration computing resources that can be procured for the County. Kern County encourages the use of cloud services once the interoperability, portability, security standards, and guideline requirements are satisfied. For specifics on the service requirements refer to the Information Technology Standards.
- b. Cloud solutions that will be utilized should be FedRAMP approved. Solutions that have not been through the FedRAMP approval will be vetted by Risk Management, County Counsel, and Deputy CITO.
- c. Cloud communication shall comply with current laws, regulations, and County policies.
- d. Cloud solutions shall be approved by the Department Head and ISO to ensure the Kern County Technology standards and security measures have been met.

720. Provision for Purchase and Internal Development.

- e. Identify security requirements when developing specifications for any information systems. Include these requirements in appropriate design or RFP documentation.
- f. Ensure all security requirements meet Kern County Standards and applicable regulations.

721. Acceptance of Risk and Responsibility.

.1 The security of the County's information technology resources and information is the responsibility of all County employees.

.2 Information security risk decisions are assigned to, and are the responsibility of the County departments whose information is the target of the particular risk. When presented with an approved security risk assessment of an existing or proposed change or service, information owners shall review the risks to their information technology resources and information from the identified security risks and security gaps, and either:

- a. Accept the risks to their information and provide written documentation the risk has been accepted when there is a known potential impact; or
- b. Execute Information Security's recommendations and/ or other mitigation steps in order to reduce the risk to an acceptable level; or
- c. Transfer the risks to another entity (such as a third party contact).

.3 The Department head, their designee, and/or the County Board of Supervisors shall be responsible for any information or information technology resource risk decision where the risk applies to a significant portion of a department or to the entire County as a whole.

722. Enforcement. Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

**KERN COUNTY ELECTRONIC COMMUNICATIONS USAGE POLICY**

**Issue Date: March 8, 2005**

**Revision Date: February 13, 2018**

**I. Purpose**

- A. To provide a policy that defines conditions for the authorized use of information technology and associated electronic information devices, including, but not necessarily limited to, the following:
- E-mail (electronic mail)
  - Text Messaging
  - Portable Device Photos
  - Instant Messaging (Skype, Hangouts, WhatsApp etc.)
  - Internet use
  - Telephone and voice-mail
  - Video conferencing
  - Desktop computers
  - Laptop computers
  - Cellular phones
  - Personal Digital Assistant (PDA)
  - FAX
  - Diskettes and other storage media
  - Online bulletin boards
  - Television
  - Electronic documents
  - Pagers
  - Copy Machines
  - Any other forms of electronic communication.
- B. County employees, contractors, or vendors with access to Kern County electronic communications are required to abide by this policy while using the County's data and telecommunications infrastructure. All references to County employees throughout this document shall also apply to all contractors, vendors and other non-County employees who have been granted access to County owned electronic communications. All County employees, contractors, or vendors using the County's data and telecommunications infrastructure must sign the acknowledgment on the last page of this document.
- C. These are considered minimum guidelines. Department Heads may develop stricter policies for their department.

**II. General Principles**

- A. Electronic communications services are provided by Kern County to support open communications and research through the exchange of information and to provide the opportunity for collaborative government-related work. Kern County encourages the use of electronic communications by its agencies and employees.

- B. The County's electronic communication systems are the property of Kern County government and are intended for use in carrying out government business. Kern County retains all personal property rights in any matter created, received or sent via the County's electronic communications systems and such matter is not the property of the employees. The contents of any electronic communication may be disclosed to authorize individuals within the organization without the permission of the sender or recipient. ***Employees should have no expectation of privacy in any matter created, received or sent using the County's electronic communications systems.*** Employees must not assume that communications or messages of any type are confidential because a private password is used. The use of passwords to gain access to the electronic communications systems is for the protection of the County, not employees. The appropriate County staff must have access to the entire network.
- C. Electronic communications are "public records" under Government code section 6253.9 (part of the Public Records Act) that provides essentially that even though records are in electronic format they are still subject to review and inspection by the public.
- D. Although access to information and information technology is essential to the missions of government agencies and their employees, ***use of electronic communications services is a revocable privilege.*** Conformance with acceptable use, as expressed in this policy statement, is required. All Kern County departments are expected to maintain and enforce this policy.

### III. **Applicability**

- A. All Kern County employees shall be covered by this policy.
- B. Contractors and other non-County employees may be granted access to County-provided electronic communications services at the discretion of the contracting authority. Acceptable use by contractors and other non-County employees working for Kern County is the responsibility of each department's contract monitor. The contract monitor is expected to provide contractors who use Kern County electronic communications services with this information.

### IV. **Policy**

#### A. **Scope**

1. This policy applies to all electronic and telephonic communications systems and all communications and information transmitted by, received from, or stored in these systems. These systems are the property of Kern County, and as such, are to be used primarily for job-related communications.
2. While in the performance of work-related functions, while on the job, or while using publicly owned or publicly provided information processing resources, employees are expected to use those resources identified in Section I responsibly and professionally and shall make no intentional use of those resources for any unlawful purpose.
3. Employees may make reasonable personal use of publicly owned or provided resources as long as:



- a. There is no or negligible cost to the County or public;
  - b. There is no negative impact on employee performance of public duties;
  - c. Employees shall reimburse the County if any costs are incurred; and
4. No other provision in this Usage Policy is violated, including that which prohibits intentional use of resources for an unlawful purpose.
  5. All County rules, regulations, and guidelines, as they presently exist and as they may be amended in the future, on ethical and appropriate behavior of County employees and the appropriate use of County resources apply to the use of all electronic communications.

## **B. Enforcement**

Department Heads or their designated representatives are responsible for disseminating and enforcing their employees' compliance with the provisions of this policy and for investigating non-compliance. When an instance of non-compliance with this policy is discovered or suspected, the agency shall proceed in accordance with departmental and Kern County personnel policies. Employee's privileges may be revoked when deemed necessary to maintain the operations and integrity of Kern County information systems. User access, accounts, passwords, software and hardware may be withdrawn without notice if an employee is suspected of violating this Electronic Communications Usage Policy. Employee discipline may be appropriate in cases of non-compliance with this policy. Criminal or civil action against employees may be appropriate where laws or rights are violated.

*Employees need to know that any electronic media communication may be considered a public record subject to disclosure under California law.*

## **C. Acceptable Uses:**

1. Communication and information exchange directly related to the mission or work tasks of the County department.
2. Communication and exchange for professional development, to maintain currency of training or education, or to discuss issues related to the employee's department activities.
3. Applying for or administering grants or contracts for County research or programs.
4. Advisory, standards, research, analysis, and professional society activities related to the County governmental work tasks and duties.
5. Announcement of new laws, procedures, policies, rules, services, programs, information, or activities.
6. All Kern County business conducted electronically should occur via County owned servers and/or devices. Kern County will respect the privacy of an employee's voluntary use of personally owned devices to access Kern County resources. A registered device for multi-factor authentication (MFA) is not communicating County data or resources. Use of a personal device for MFA is to gain access to the County network. In the event of a request for public records or other legal means of obtaining County records, the

employee is required to provide those records if they reside on an employee's personal device and sign an acknowledgment that all information was provided pursuant to the request.

**D. Prohibited Uses:**

Electronic media and communications shall not be used in any manner in violation of the law or County rules, policies or procedures. Electronic media and communications shall in no manner be used for any improper, illegal, offensive or harassing purpose. Activities prohibited by this policy include, but are not necessarily limited to the following:

1. Accessing or sending of any material or communication in violation of any federal, state, or local law, ordinance, or regulation.
2. Accessing or sending of any material or communication which includes potentially offensive material (such as pornography, or sexual, racial or ethnic comments, jokes or slurs).
3. Accessing or sending any material of a political nature is prohibited. Employees may not use County time and equipment to either support or oppose campaigns or candidates for elected offices. Messages of a religious nature or promoting or opposing religious beliefs will not be allowed.
4. Using e-mail to send information that needs to be communicated individually to every County employee (several hundred employees do not have access to a computer on a regular basis), or if a quick response is needed. Many employees may not or cannot check their electronic mail on a frequent basis. When establishing or changing a policy, formal policies should be announced via a memo instead of e-mail.
5. Misrepresentation under any circumstances of an employee's true identity.
6. Unauthorized access to any computer system.
7. Any action intended to accomplish or assist in unauthorized access to computer systems.
8. Unauthorized or improper downloading, accessing or sending of copyrighted information, documents or software.
9. Personal Web Sites. County employees are prohibited from developing and running personal Web sites on County electronic communications equipment or on or through any County contracted ISP services.
10. Use of County's electronic communications equipment or network for private business purposes, including non-profit, charitable and for profit businesses.
11. Use of County electronic communications equipment or network for any purpose related to gambling.
12. Purchases through the County's electronic communications networks. Employees shall not use the County's access to purchase, obtain or offer products or information for County purchases without prior approval through normal Kern County Purchasing Procedures.
13. Sending of unauthorized broadcast communications or solicitations (such as a County wide e-mail message). The Department Head or their designated representative must approve all County wide broadcast or solicitation messages in advance.
14. Any action that causes the County to incur a fee for which there has not been prior approval.
15. Use of a security code or password other than as authorized.

16. Disclosing a username and password to anyone for any purpose.
17. Sending confidential communications via e-mail. Common sense should be employed if a communication must be kept confidential. Information dealing with personnel issues may lose confidentiality due to its electronic transmission. It is recommended that confidential or other sensitive materials not be transmitted electronically.
18. Streaming Audio, Video and Data. Electronic communications networks are a shared resource. Although watching KGOV is acceptable, listening to the radio is not. Also prohibited are any stock market, weather, sport or other types of streaming data tickers. The Department Head or their designated representative must approve all uses of streaming audio, video and data in advance.
19. Employees may not use any non-County web site which requires the acceptance of any contractual terms and conditions as a condition to use that web site without prior Department Head and/or Counsel approval.

#### **E. Notice of County's Rights:**

Employees need to be aware that deleting electronic communications – e.g., deleting an e-mail message from their mailbox or voicemail from their Audix– does not necessarily mean that they are permanently deleted from the system. In the case of e-mail and voice mail messages, these messages may be saved by the County and employees should have no expectation of privacy in any electronic media communications. Employees should further be advised that the County maintains a record of all telephone usage regarding all incoming/outgoing telephone calls including the date/time of the call, duration of the call, and the incoming and outgoing phone numbers. This usage information is subject to Public Disclosure and/or subpoena by the Courts.

All electronic media communications are considered at all times to be County records. The County has the capability to access, monitor, review, and copy or disclose any electronic media communications; and the County reserves the right to do so for any proper County purpose. The use of security measures (such as individual passwords) or deletion of electronic media communications (such as deletion of e-mail messages by employees) does not affect the County's ability or right to access, review, copy or disclose such communications under appropriate circumstances. Employees' use of electronic media is consent to such action by the County.

This policy shall not be interpreted to limit the County's access to electronic media communications under appropriate circumstances; and shall not in any way limit the County's control or ownership of its electronic media systems. However, this policy is in no way intended to permit unauthorized access to electronic media communications.

#### **F. Software:**

1. Employees shall use only legally acquired and licensed software distributed by the department and approved in accordance with Chapter 7 of the Administrative Procedures Manual. The Software Licensing and Use Policy key provisions are summarized below:
  - a. Only properly licensed and/or registered software will be loaded on County-owned computers.
  - b. Software acquired at County expense shall not be copied onto any non-County computer unless specifically authorized by the license agreement.

- c. Departments shall establish a permanent file that documents the right to use each copy of the software loaded on a County computer.
- d. Departments shall audit their computers at least annually to ensure compliance with all licensing requirements.

Downloading software is prohibited without prior approval by the Department Head or their designated representative.

2. Loading any program or data from diskette, CD, tape or other portable media into a County owned computer or other device when such media has not been scanned by anti-virus software.
3. Employees must get the approval of the Department Head or their designated representative prior to loading County owned software with home use options on home computers and must abide by this policy while using them.

## **G. E-mail, Text Messages, and Other Electronic Communications**

### **1. Retention of Official Records Required**

Any e-mail, text message, or other electronic communication that is an “official record” must be retained. “Official record” means any record that constitutes a lasting indication of a writing, event, or other information, and:

- a. Is prepared or received or required to be retained pursuant to a State or federal statute, regulation, or case law; or
- b. Is required to be retained by the records retention schedule adopted by the Board of Supervisors; or
- c. Is necessary and convenient to the discharge of a public officer’s duties and was made or retained for the purpose of preserving its informational content for future reference.<sup>1</sup>

Examples of electronic communications that constitute “official records” that must be retained:

- E-mails related to policy or decision-making
- E-mails connected to specific case files
- E-mails that relate to contracts
- Other e-mails that are an essential part of a larger record, or other memorandum of significant public business.

Examples of electronic communications that are not “official records” subject to retention:

- E-mails announcing only the date and time of a meeting;
- Personal messages not related to County business.

### **2. Retention Requirements**

---

<sup>1</sup> See Administrative Bulletin No. 11: Retention and Destruction of County Records, Definitions.

a. E-mails Sent From or Received on County Accounts

The County shall maintain an archive that retains all e-mails sent from or received on County e-mail accounts for two years from the date of sending or receipt. The employee or official who possesses an e-mail on their County account shall preserve the e-mail beyond the two-year time period if any of the following applies:

- i. The e-mail is subject to a current California Public Records Act request;
- j. The e-mail is related to pending litigation; and/or
- k. The e-mail is an official record that is subject to a longer retention period under Administrative Bulletin No. 11: Retention and Destruction of County Records.

b. E-mails Sent From or Received on Private Accounts

Any employee or official who sends or receives an e-mail that is an “official record” on their private account shall immediately forward that e-mail to their County e-mail account.

c. Text Messages

Any employee or official who sends or receives a text message that is an “official record” on either a County-owned or a private device shall immediately forward the text message to their County e-mail account.

d. Photographs on Cellular Devices

Any employee or official who takes a photograph that is an “official record” on either a County-owned or a private device shall immediately send the photograph to their County e-mail account.

### **3. Additional Electronic Communications Guidelines**

- a. The responsibility for compliance with this policy lies with each County employee. It is the responsibility of departmental management to develop internal procedures consistent with this policy to ensure compliance.
- b. Employees need to know that even when they delete an e-mail or voice mail from their mailbox (and empty it from their Trash or equivalent), it may continue to exist in backup or archival storage devices or in the mailboxes of other recipients or addressees.
- c. If an employee sets up a vacation rule that generates an automatic reply to incoming e-mails:

The reply option should always be “reply to sender”, not “reply to all”. The “reply to all” option can cause problems if the original e-mail was sent to a large group of people. The rule should be set up to reply only to messages where the From field does not contain an “@” symbol. (so that the rule will NOT reply to messages originating outside of the County.) The reason for this setting is that if the original e-mail was sent from an automated

system, the vacation rule reply will sometimes trigger it to resend the original message each time it gets a reply, causing a loop that can flood the mailbox with messages and overburden the County's e-mail infrastructure.

- d. Employees shall only access e-mail accounts through systems set up by the County, including Office and Exchange (Courts). Employees shall not access hotmail.com and similar e-mail accounts via an Internet connection over the Wide Area Network (WAN). It has been detected that these types of e-mail accounts bypass the County's security network and make the County's WAN vulnerable to viruses.

#### **H. Additional Guidelines:**

1. Logoff (Exiting). Always make a reasonable attempt to complete the logoff or other termination procedure when finished using any system such as Internet, GroupWise, etc.
2. Large File Transfers and Network Capacity. Electronic communications networks are a shared resource. While routine electronic mail and file transfer activities won't significantly affect other users, large file transfers will impact the service levels of other users. Employees contemplating file transfers over 10 megabytes per transfer should schedule these activities before or after regular business hours.
3. Certain electronic media (especially e-mail) may not be appropriate to transmit sensitive materials, which may be more appropriately communicated by written document or personal conversation.
4. Employees should always remember that persons other than the sender and the recipient may read electronic media communications at a later date. Accordingly, electronic media communications (such as e-mail messages) should always be treated as written memos, which may remain on file in various locations.

#### **I. Requests for Electronic Data:**

Requests to produce copies of or provide access to non-routine information from electronic communication systems shall immediately be forwarded to the appropriate

Department Head. Upon review the Department Head can determine if County Counsel should be contacted.

#### **V. Written Acknowledgment:**

Department Heads shall have all employees acknowledge in writing that they have received and read this policy. Such written acknowledgment shall be retained in department files. (Nevertheless, the failure to provide such written acknowledgment shall not in any way limit the County's ability to enforce this policy.)



# KERN COUNTY TECHNOLOGY STANDARDS

Approved April 2017  
Revised June 14, 2022

# Table of Contents

- 1. Network Equipment..... 2
- 2. Servers..... 5
- 3. Workstations..... 6
- 4. Laptops..... 7
- 5. Tablets..... 8
- 6. VoIP (Voice over IP)..... 9
- 7. Data Storage..... 11
- 8. Wireless..... 13
- 9. Operating System and Software ..... 17
- 10. Email System ..... 19
- 11. Mobile Devices ..... 21
- 12. Development Tools ..... 23
- 13. Security Standards ..... 27
- 14. IT Media ..... 32
- 15. Virtualization..... 34
- 16. Cloud Standards ..... 36
- Appendix A: Cloud Request for Services and Approval.....43



# 1. Network Equipment

For the purposes of this document, a router is defined as a device that provides connectivity between subnets and is connected in any way to the County WAN. Devices or software that provide routing capabilities as a secondary function – e.g., firewalls – are not considered to be routers in this context.

Routers, Layer 3 Switches, Layer 2 Switches, Firewalls, and CSU/DSU

Routers forward data packets along two or more network subnets. A Legacy T1 Router is described as a router that connects two network subnets over the WAN typically provided by an ISP's network (i.e. T1's, 56k links). Routers are located at edge networks and act as gateways between two or more Networks. Legacy T1 Router utilizes an internal or external CSU/DSU to translate the network protocols into appropriate frames to the ISP's wide-area network.

- Layer 3 switch can perform routing functions in addition to switching by performing intelligent packet forwarding (routing) based on Layer 3 information.
- Layer 2 Switch uses hardware interlinks and Media Access Control (MAC) addresses to forward packets to the correct hosts. A Layer 2 Switch provides the same functions as a Layer 3 Switch without enhanced capabilities.
- CSUs/DSUs (Channel Service Unit/Data Service Unit) are defined as devices that connect LANs to WANs, generally via a T-1/digital circuit interface.

## 1. All Device Types Standards

- a. All devices will be inventoried to include: management IP address, model, firmware version, warranty information and identify if the device is end of life
- b. Diagrams will be updated and maintained to include all devices and connections.
- c. Network devices will be stored in a secure location.
- d. Emergency/ Management accounts will be documented and stored in a secure location.
- e. Passwords will comply with the Information Security policy.
- f. A deny by default security posture should be implemented for traffic entering and leaving the network segment.
- g. Configurations of the device should be copied and stored in a secure location.

## 2. Layer 2 Switch Standards

A Layer 2 Switch uses hardware interlinks and Media Access Control (MAC) addresses to forward packets to the correct hosts. A Layer 2 Switch provides the same functions as a Layer 3 Switch without capabilities.

- a. Capabilities include:
  - QOS
  - SNMP v3 compatible
  - Dedicated management port (e.g. USB, serial port, console port)
  - Spanning tree
  - Secure Remote administration capability (e.g. SSH, HTTPS)
  - Port Mirroring
  - Must have current maintenance contract or keep spare units in stock
  
- b. Unmanaged Switch Capabilities include:
  - The device may not be used as an uplink to more than a single Layer 2 or Layer 3 switch.
  - The device should be used as an endpoint to provide expanded Ethernet ports for end-user devices such as PCs, printers, or mobile devices.
  - All unmanaged switches need to be tracked on an inventory list.
  
3. CSU/DSU Standards

All external connections will be documented and reviewed on an annual basis for business need.
  
4. Cable and Cable Installation Standards
  - New or upgraded LAN installations must be Fast Ethernet at a minimum.
  - All new copper cable installation must be Gigabit rated cable.
  - All new fiber optic cable installations must be multimode cable for LAN installations, except that single mode should be installed for long distance data and video transmissions.
  - All contracts for cable installation, regardless of cable type, must include a requirement that the installation meet or exceed the applicable IEEE industry standards, and require that test results be provided.
  
5. Layer 3 Switches Standards

A Layer 3 switch is an enterprise-grade device that can perform routing functions in addition to switching by performing intelligent packet forwarding (routing) based on Layer 3 information. The hardware inside a Layer 3 switch merges that of traditional switches and routers, replacing some of a router's software logic with hardware to offer better performance.

  - a. Required Minimum Features
    - QoS
    - SNMP v 3 compatible
    - Dedicated Management Port (i.e., USB, serial port, console port, etc...)

- Secure Remote administration (i.e., SSH, https, etc...)
- Port Mirroring
- Must have current maintenance contract (to receive security updates)
- Must support industry-standard routing protocols (i.e. RIP, static routes, OSPF, etc...)

b. Interoperability

A Layer 3 Switch that interfaces directly with another County department's network must be agreed upon by all interested parties to ensure interoperability.

c. Warranty and Maintenance

Since Layer 3 switches are often deployed as core networking devices for departments, a premium maintenance agreement must be purchased for the life of the device or spare equipment with ability to download security/update patches.

d. Replacement

Layer 3 switches should be replaced when vendor support is no longer available or cost prohibitive.

e. Approved Vendors

- Avaya preferred
- Cisco

6. Legacy T1 Router

Note: A Legacy T1 Router is described as a router that connects two network subnets over the WAN typically provided by an ISP's network (i.e. T1's, 56k links). Routers are located at edge networks and act as gateways between two or more Networks. Legacy T1 Router utilize an internal or external CSU/DSU to translate the network protocols into appropriate frames to the ISP's wide-area network

a. Approved Manufacturers

- Avaya is the preferred standard
- Cisco
- 

b. Justification

These Manufacturers have been chosen because they have been tested and approved. There are more router manufacturers out there but for troubleshooting and compatibility reasons we would like to narrow them down these three.

c. Standards

The standards have been implemented to reflect a secure and optimal operating environment. All devices should be maintained and purchased to at a standard level. For devices that are legacy and do not meet the requirements of the standard

should be documented and present a plan to upgrade the equipment. The legacy devices should be monitored to ensure there are no compromised incidents. The manufacturers selected have been tested throughout the county to ensure interoperability with different technologies and designs.

d. Warranty and Maintenance

All Devices must be leased or purchased with either:

1. A premium maintenance agreement for the life of the equipment, or
2. Depot maintenance agreement and/or spare equipment for replacement.
3. All devices must hold a current maintenance contract.

e. Life Cycle

The device should be replaced when vendor support is no longer available, or is cost prohibitive. If there is a device that is end of life and needs to continue to be operational written approval needs to be provided by the Department Head (or their representative) and the Deputy Chief Information Technology Officer (Deputy CITO).

## 2. Servers

a. Standards

1. Maintain an up-to-date inventory list with the end-of-life schedule.
2. Servers that are decommissioned or removed will clean all data from the hard drives with a wiping utility, or destroyed until completely unreadable.
3. Business critical hardware should have a secondary sustainable power source.

b. Justification

The server class requirement ensures that the hardware is designed for heavy network and 24x7 use. The requirements include the growth of new technology requirements and capability to sustain the increase in data.

c. Manufacturers

1. Dell, HP, IBM
2. Non Intel/ AMD based (e.g. AS/400 servers)
3. The choice of enterprise server is generally dictated by the application. For that reason, no specific manufacturer is recommended.
4. Intel/ AMD based
5. Departments with In-House Technical Support Staff. These departments should purchase or lease a production server manufactured by a preferred company unless a recognized exception applies.

6. Departments without In-House Technical Support Staff. These departments must follow ITS specifications
- d. Minimum Specifications
    1. Server class machines required regardless of the choice of manufacture, only a server class machine may be purchased for use as a production server, unless a recognized exception exists.
    2. Follow the vendor and best practices for recommended processor, RAM, and hard ware specifications. If there are any questions refer to ITS for verification of specifications.
  - e. Warranty and Maintenance

All enterprise production servers should be purchased or leased with an applicable maintenance agreement for the service life of the server. Notification of exceptions will be provided to the Deputy CITO.
  - f. Life Cycle

Enterprise servers should be replaced every 7 years unless end of life by the vendor. If there is an enterprise server that is end of life and needs to continue to be operational written notice needs to be provided to the Department Head (or their representative) and the Deputy CITO.

### **3. Workstations**

- a. Standards
  1. Maintain an up to date inventory list with the end of life schedule.
  2. Workstations that are decommissioned or removed will clean all data from the hard drives with a wiping utility, or destroyed until completely unreadable.
- b. Justification

Standardizing increases the efficiency of technical staff and ensures reliable and adequate technical support. The business class requirement ensures that the hardware is designed for network and 8 hour/ day use.
- c. Manufacturers
  1. Dell, HP, Lenovo
  2. Departments with In-House Technical Support Staff

These departments must purchase or lease desktop computers manufactured by hardware manufacture that provide Tier III support.
  3. Departments without In-House Technical Support Staff

4. These departments must follow ITS specifications

d. Minimum Specifications

1. Minimum specifications need to meet the recommended requirements for the operating system and intended applications.
2. Business Class Requirement. Desktop computers must be business class machines specifically manufactured for installation in a network and must be certified by the manufacturer for the appropriate network client software.

e. Warranty and Maintenance

Maintenance for desktop computers should be leased or purchased with applicable maintenance for the life of the equipment.

f. Life Cycle

Desktop computers should be replaced after no more than five years of service.

## 4. Laptops

a. Standards

1. Maintain an up to date inventory list with the end of life schedule.
2. Laptop that are decommissioned or removed will clean all data from the hard drives with a wiping utility.

b. Justification

Standardizing increases the efficiency of technical staff and ensures reliable and adequate technical support. The business class requirement ensures that the hardware is designed for network and 8 hour/ day use.

c. Manufacturers

1. Dell, HP, Toshiba, Lenovo, Acer, ASUS
2. Departments with In-House Technical Support Staff
3. These departments must purchase or lease laptops manufactured by hardware manufacture that provide Tier III support.
4. Departments without In-House Technical Support Staff. These departments must follow ITS specifications.

d. Minimum Specifications

1. Processor and System Memory. Because processing requirements greatly depending on how the laptop is being deployed, no standards are specified in this area.
2. Business Class Requirement. Laptops must be business class machines specifically manufactured for installation in a network and must be certified by the manufacturer for the appropriate network client software.

- e. **Warranty and Maintenance**  
Laptop computers must be leased or purchased with a minimum of three years' warranty.
- f. **Life Cycle**  
Laptop computers must be replaced after no more than five years of service.

## 5. Tablets

- a. **Standard**
  - 1. Maintain an up to date inventory list with the end of life schedule.
  - 2. Tablet PC that are decommissioned or removed will be reset back to manufacturer default.
- b. **Justification**  
Standardizing increases the efficiency of technical staff and ensures reliable and adequate technical support. The business class requirement ensures that the hardware is designed for the support of a user working outside of the business office.
- c. **Manufacturers**
  - 1. Apple, Dell, HP, Microsoft, Lenovo
  - 2. Departments with In-House Technical Support Staff  
These departments should purchase or lease tablet PC manufactured by hardware manufacture that provide Tier III support.
  - 3. Departments without In-House Technical Support Staff. These departments must follow ITS specifications.
- d. **Minimum Specifications**
  - 1. Apple will be covered under the latest hardware recommended by Apple.
  - 2. Android hardware should be able to handle the latest operating system version.
  - 3. Windows tablets hardware will be able to support the full version of the operating system.
- e. **Warranty and Maintenance**  
Tablets should be leased or purchased with applicable maintenance/warranty for the lifetime of the device or as practical.
- f. **Life Cycle**  
Tablet computers should be replaced after no more than five years of service.

## 6. VoIP (Voice over IP)

Refers to the transmission of speech across data networks vs the traditional method of a dedicated wire from the phone system to the phone utilizing TDM (time division multiplexing) for digital phone sets. This technology allows the transmission of speech to be shared with the transfer of data on the same wire. This convergence of networks allows for a less complicated physical network, but it does complicate the logical network.

Kern County currently has 3 main Avaya telephone systems that deliver service to various offices throughout the county. These 3 systems are located at 1115 Truxtun Ave, 100 East California Ave and 1700 Mt Vernon Ave. These systems are a mixture of VoIP and TDM technology that provide phone service for county employees.

Along with the 3 main phone systems, there are also 3 voice mail systems which are also provided by Avaya. Voice mail and the phone systems are integrated to provide not only basic functionality, but also provide Avaya specific features which all county phones share.

Seeing that Avaya phone systems are predominantly used in the county, it allows the county to streamline support, integration, common phone sets that can be interchanged between locations and changes to the system. This integration would be more difficult if another phone system vendor was introduced into the Avaya environment and possibly restrict full interoperability.

As of the date of this writing, there is no set date as to when TDM technology has to be completely removed from all locations and restricting use to VOIP only.

### a. Standards

Basic functions of a VoIP network design consist of the following major components:

- Routers
- Switches
- Phone system gateway/servers
- Voice Mail

### b. Routers

Routers need to provide a basic set of functionality (as defined in routers standards document) that would ensure proper functionality with other devices that it connects too. This functionality would also include the ability to provide Quality of Service (QoS) queues that would be able to ensure that voice traffic is delivered as a higher priority over other data traffic, as it passes through the router. The router needs to also have the ability to tag the traffic utilizing DSCP (differentiated services code point) which assigns the traffic to a particular QoS queue. The size of the router, as



well as the bandwidth/speed, is determined on a case by case basis. There are several factors that need to be considered such as:

1. Number of users at the location.
2. Services provided and overall utilization.
3. Other data related equipment such servers providing local storage, email and printing.

c. Switches

1. Switches need provide a basic set of functionality (as defined in the switches standards document) as well as have the ability to provide power to the phone set using a feature call PoE (power over Ethernet). If the location is relatively small and there are only a few phones at the location, this requirement can be waved and the power for the phone set can be a local power supply at the desktop.
2. Size (port density) and speed (packets per second) of the switch is determined by the amount of users at that location as well as other related data equipment attached to the switch.

d. Phone system gateway/servers

Avaya is the preferred vendor that provides phone equipment to the County of Kern. This has been beneficial for several reasons.

1. Several departments have received the same training and are able to help support one another on technical issues that have surfaced.
2. The county is able to have a master support agreement in place that covers all Avaya phone systems.
3. Phone sets are compatible with one another at various locations.
4. The County is able to maintain a stock of commonly used parts.
5. Integration and interoperability is much easier to achieve and maintain when utilizing one vendor (such as Avaya).
6. Adding new equipment (gateway local to the location) into the network is streamlined because of the existing compatibility.

e. Voice Mail

The County Voice Mail system is provided by Avaya and is fully integrated with the current County phone system. The advantages of keeping with one vendor for Voice Mail and Phone system equipment is the same as the benefits listed above for phone system equipment.

f. Justification

Avaya phone systems are predominantly used in the county; it allows the county to streamline support, integration, common phone sets that can be interchanged between locations and changes to the system. This integration would be difficult with a vendor mixed environment and possibly restrict full interoperability.

g. Approved Solutions

- Avaya

## 7. Data Storage

Note: For the purposes of this section, data storage is defined as system of disk, solid state, tape or other devices designed to provide persistent and reliable access to data. Data storage systems include, but are not necessarily limited to direct-attached storage (DAS), network-attached storage (NAS), storage area networks (SAN), tape backup systems, disk-based backup systems, and hybrid disk/solid state appliances.

### a. Standards

#### 1. Storage

Due to the quickly-evolving landscape of storage technology, no IEEE standards or RFCs exist to define data storage devices, appliances and components. All storage vendors have proprietary features and components in their product lines. The purpose of this standard is to provide guidance for departments on minimum capabilities and features they should seek out when purchasing storage equipment for their organization.

#### 2. Vendors

- Dell Compellent

### b. Encryption

It is recommended that applications and data be encrypted at the server level, instead of at the storage device. It is the responsibility of the Department to ensure that their applications meet any regulatory or legal requirements for encryption.

### c. Storage-Area Networks (SAN)

Definition: A storage area network (SAN) is a dedicated high-speed network that interconnects shared pools of storage devices to multiple servers. A SAN moves storage resources off the common user network and reorganizes them into an independent, high-performance network. Servers can access data on the SAN as block-level logical units (LUNs) which appear and perform like locally-attached storage.

### d. Minimum capabilities

Due to the expense of an enterprise-grade SAN, it is advised that users only consider this option for the most important of mission-critical applications. Some of these applications include server virtualization and virtual desktop infrastructure

(VDI) when choosing a SAN, departments should look for the following minimum features:

1. **Redundant drive controllers**  
To provide maximum uptime and redundancy in the event of component failure, a SAN should have at least two drive controller units.
2. **Redundant network fabric and pathways**  
To provide for maximum uptime in the event of network component failure, a SAN should have at switching with network pathway failover capability.
3. **SAN Protocols**  
Depending on the level of performance required for the desired application, a SAN should support the iSCSI, Fiber Channel (FC) and/or Fiber Channel over Ethernet (FCoE) protocols.
4. **Snapshot/Replay features**  
The ability to roll back LUNs to previous states in the event of data loss or other failure is key to maintaining high levels of availability/
5. **Management capabilities**  
The SAN should provide a central application to control and manage LUNs, snapshots and secure access to the SAN.
6. **Maintenance Contract**  
Departments should purchase a maintenance and support contract for the life of the product. If the product is intended to run a mission-critical application, departments should purchase a contract with a premium service level agreement (SLA) which requires the product to receive service within a four (4) hour window.

e. **Network Attached Storage (NAS)**

Definition: Network Attached Storage (NAS) refers to servers and disk arrays attached to a network by Ethernet. NAS devices typically provide file-level storage, although some devices also provide block-level access via the iSCSI protocol. NAS is differentiated from SANs by the lack of Fiber Channel interconnects.

1. **Minimum Capabilities:**  
Departments are advised to specify the redundancy and management capabilities they need to ensure that their application needs are met by the device. At a minimum, devices should support redundancy through RAID 5.
2. **Maintenance Contract:**

Departments should purchase a maintenance and support contract for the life of the product. If the produce is intended to run a mission-critical application, departments should purchase a contract with a premium service level agreement requiring same-day service turnaround.

f. **Direct-attached Storage (DAS)**

Definition: Direct-attached storage (DAS) refers to devices that attach directly to a server via Serial Attach SCSI (SAS), Fiber Channel or other direct means as opposed to connect through a network protocol.

1. **Minimum Capabilities**

Departments are advised to specify the redundancy and management capabilities they need to ensure that their application needs are met by the device. At a minimum, devices should support redundancy through RAID 5. Most DAS devices also support redundant drive controllers.

2. **Maintenance Contract**

Departments must purchase a maintenance and support contract for the life of the product. If the produce is intended to run a mission-critical application, departments should purchase a contract with a premium service level agreement requiring same-day service turnaround.

## **8. Wireless**

a. **Purpose**

This policy establishes standards that should be met when wireless communications equipment is connected to Kern County networks. The policy prohibits access to Kern County networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by the Department of Information Technology Services are approved for connectivity to Kern County's networks.

b. **Scope**

This policy covers all wireless data communication devices (e.g., personal computers, phones, PDAs, etc.) connected to any of Kern County's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Kern County's networks do not fall under the purview of this policy.

c. **Policy**

Approved equipment brands – Avaya preferred, Cisco

All wireless LAN equipment should be evaluated and approved by the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) publication 140-2 or by the Common Criteria. If the wireless LAN equipment is not approved in both the NIST FIPS 140-2 and the Common Criteria, a formal waiver request for the purchase of the wireless LAN equipment should-be

generated, sent, and approved by the Kern County Deputy Chief Information Technology Officer (Deputy CITO.)

1. (<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>)
2. (<https://www.commoncriteriaportal.org/products/>)
3. All equipment should have a current maintenance agreement.
4. Equipment firmware and IPS definitions should be kept current.

d. Monitoring of uncontrolled wireless devices

1. All locations where wireless data networks are installed will be equipped with sensors or systems to automatically detect, classify, and disrupt communication with unapproved wireless access points.
2. All locations where wireless data networks are installed will be equipped with sensors or systems to automatically detect the presence of wireless devices forming a connection between the wired network and any wireless network. This would include laptops that are serving as a bridge between wired and wireless networks.
3. In locations where wireless LAN access has been deployed, wireless intrusion detection systems will also be deployed to monitor for attacks against the wireless network. The wireless intrusion detection system should be integrated with the wireless LAN access system whenever possible.

e. Authentication of wireless clients

1. All access to wireless networks must be authenticated.
2. The County's existing strong password policy must be followed for access to wireless networks.
3. The strongest form of wireless authentication permitted by the client device must be used. WPA2 with 802.1x/EAP-PEAP or 802.1x/EAP-TLS must be used as a minimum.
4. Where 802.1x authentication is used, mutual authentication or server authentication must be performed. Client devices must validate that digital certificates presented by the authentication server are trusted and valid. Under no circumstances may clients disable validation of server certificates and blindly trust any certificate presented. EAP methods that do not support certificate-based mutual authentication or server authentication may not be used.
5. EAP methods that exchange authentication credentials outside of encrypted tunnels may not be used. These methods include EAP-MD5 and LEAP.
6. When legacy devices that do not support 802.1x/EAP-PEAP or 802.1x/EAP-TLS must be used on a wireless network, they will be isolated from all other wireless devices and will be restricted to the minimum required network access. Violations of the configured rules, indicating that an intrusion has taken place, must cause the device to be immediately disconnected and blocked from the network.

g. Encryption

1. All wireless communication between County devices and County networks must be encrypted. Wireless networks providing only Internet access for guest users are exempted from this requirement.
  2. The strongest form of wireless encryption permitted by the client device must be used. With a min of WPA2 using AES-CCM encryption must be used.
  3. Client devices that do not support WPA2 should be secured using VPN technology such as IPSEC.
- h. Access control policies
1. Access to County network resources through wireless networks should be restricted based on the business role of the user. Unnecessary protocols should be blocked, as should access to portions of the network with which the user has no need to communicate.
  2. Access control enforcement shall be based on the user's authenticated identity, rather than a generic IP address block. This is also known as "identity-based security."
  3. The access control system must be implemented in such a way that a malicious inside user is unable to bypass or circumvent access control rules.
- i. Client security standards
1. Where supported by the client operating system, it is recommended the wireless network will perform checks for minimum client security standards (client integrity checking) before granting access to the County network. Specifically:
  2. All wireless clients must run County approved anti-virus software that has been updated and maintained in accordance with the Company's anti-virus software policy.
  3. All wireless clients must have security-related operating system patches applied that have been deemed "critical" in accordance with the County's security policy.
- j. Wireless guest access
1. Wireless guest access can be available at facilities where wireless access has been deployed.
  2. Wireless guest user traffic is separated via VLAN or physical network separation from the County traffic and is routed to a separate internet connection.
  3. All wireless guest access will be authenticated through a web-based authentication system requiring Guests to agree to a County Usage Policy.
  4. It is recommended wireless guest access is limited only to hours of operation when Guests should be present.
  5. Wireless guest access is monitored, bandwidth usage is limited, and accessible content is controlled and monitored.
- k. Terms Definitions

Term	Definition
802.11	A set of Wireless LAN/WLAN standards developed by the IEEE LAN/MAN standards committee (IEEE 802). Also commonly referred to as "Wi-Fi."
AES-CCMP	Advanced Encryption Standard-Counter with CBC-MAC Protocol. A wireless encryption protocol specified by IEEE 802.11i. Currently regarded as the strongest form of wireless encryption. EAP Extensible Authentication Protocol. A series of authentication methods used inside 802.1x to achieve wireless authentication.
IEEE	Institute of Electrical and Electronics Engineers. An international professional organization dedicated to the advancement of technology related to electricity. The IEEE is one of the main standards bodies associated with networking technology.
IETF	Internet Engineering Task Force. Develops and promotes Internet standards, in particular those of the TCP/IP protocol suite.
IPSEC	IP Security. An IETF standard for protecting IP communication by encrypting or authenticating all packets.
LEAP	Lightweight Extensible Authentication Protocol. A proprietary protocol supported by Cisco. Systems that acts as an EAP method within 802.1x. LEAP was proven insecure in 2003 and does not comply with current security standards.
PEAP	Protected Extensible Authentication Protocol. A tunneled EAP method that uses a server-side digital certificate for server authentication and a username/password for client authentication.
VPN	Virtual Private Network. A method of building private networks on top of public networks such that the private network is protected and separate.
TLS	Protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).
WLAN/Wireless LAN	A type of wireless system based on the IEEE 802.11 series of protocols.
WPA Wi-Fi Protected Access	WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards. Products displaying the WPA logo have passed a certification program run by the Wi-Fi Alliance.
WPA2 Wi-Fi Protected Access version 2	WPA2 implements the full IEEE 802.11i standard, but will not work with some older network cards. Products displaying the WPA2 logo have passed a certification program run by the Wi-Fi Alliance.

## 9. Operating System and Software

Note: The County currently has Master License Agreements with Microsoft, Novell, SuSe Linux, and Network Associates (the producers of McAfee) which is part of the justification for recommending these brands. For the most current list of license agreements, see the Procurement section on CountyNet.

### a. All Operating Systems

1. All requirements from the Information Security Policy will be met.
2. All servers must be stored in a secure location with limited access to the servers.
3. Administrator and service accounts will be documented and stored in a secure location.
4. Passwords will comply with the Information Security policy.
5. Administrators will have a separate account to perform normal daily duties.
6. Backup of the server and the data stored on the server will comply with the Administrative Bulletin 11 or the appropriate regulation. If retention times cannot be met the Department Head and Deputy CITO need to be notified.
7. Servers will be configured to an authorized time server to synchronize time appropriately. Authorized time server would be no more than 2 stratum layers. An authorized time server that pulls time from a satellite would be 1 stratum or an authorized time server that pulls from a known time website to the enterprise time server would be 2 stratum.
8. Necessary services will be documented to maintain a baseline and unnecessary services will not be used. Telnet services will not be authorized for any newly deployed technology or not operationally required. Any exceptions will be documented with the Deputy CITO.
9. A warning banner will be displayed before logon to the device.
10. All maintenance will be scheduled and documented to confirm changes made to the system.
11. New patches, software versions and software packs will be tested and applied to the system.
12. Data at rest solutions should be applied to the device if required by specific laws and regulations (e.g. HIPAA).
13. When maintaining an image for deploying new systems. The image will include all the latest patches, software versions, and drivers.

### b. Server Operating Systems

Note: It is up to each department to determine if they wish to use/support Linux or Apple Mac technology and to ensure that applications and peripherals operate correctly.



1. Microsoft Windows Server, Novell NetWareOES/SLES, and Linux all have a place in the County's organization.
2. Microsoft is the only available platform for many specialized applications, and is also a standard server operating system.
3. NetWareOES/SLES is used by some departments to run GroupWise and is also used by some departments to run Novell ZenWorks and other Netware-specific applications.
4. Linux provides a very secure environment for Web servers and other applications, requires less powerful hardware, and has lower maintenance/upgrade costs than Windows.
5. Suse Linux/OES/SLES is supported by Novell.
6. PC Operating Systems (including desktops and laptops).
7. Microsoft Windows, MAC O/S, and Linux have a place in the County's organization.
8. Microsoft Windows is the only desktop operating system that many applications (including browser-based applications that require Internet Explorer) will run on.
9. Linux is a viable alternative for those workstations that only require software that can run on Linux (e.g., Star Office, GroupWise, Firefox browser, etc.)

c. Approved Solutions

Type	Product	Version/Edition
Server Operating System	Microsoft Windows Server	Any currently supported edition
	Novell OES/SLES	Any currently supported edition
	Linux	Any currently supported edition
PC Operating System	Microsoft Windows	Any currently supported edition
	Linux	Any currently supported edition

	Apple Mac	Any currently supported edition

d. Office Products

1. Standards

- a. The Trust bar notification for security messages will be enforced.
- b. Encryption type for password protected Office application files should be set.

2. Justification

Word processors, spreadsheets and desktop database programs should no longer be viewed as individual products. They should instead be viewed as components of an office suite, which integrates these functions into a single desktop business application.

3. Approved Solutions

Office Documents that are being shared or exchanged between County departments or with other agencies must be saved in a Microsoft Office format (.DOCX, .XLSX, or .PPTX) that can be viewed/edited in Office 2007 or higher.

## 10. Email System

Note: Enterprise-level email system suites (such as Microsoft’s Exchange, etc.) whose clients/servers will properly interface with the rest of the County’s GroupWise deployment (for busy searches, address book sync, etc.) are deemed acceptable

1. Standards

Disable unused services and protocols.

2. Justification

Novell GroupWise is currently being used by all County departments, although alternatives are now acceptable based on approved solutions below.

3. Approved Solutions

Product	Version

Novell GroupWise	Any currently supported edition
Enterprise-level Server or Software as a Service (SaaS)	Any currently supported edition, or SaaS that are FedRAMP certified and have been approved by the Board of Supervisors.

a. Email Client Software

1. Standard

Product	Version
Novell GroupWise	Any currently supported edition
Enterprise-level Client or browser application.	Any currently supported edition, or services that is secure and encrypted and have been approved by the Board of Supervisors.

2. Justification

Novell GroupWise is currently being used by all County departments, although alternatives are now acceptable based on above approved email systems and conditions but still require Board of Supervisors and TAC approval.

b. Browser Software

1. Standards

- None

2. Justification

- None

3. Approved Solutions

All browsers supported by the Department's IT Staff are allowed. See the Development Standards Section for County application compatibility (browsers used not compatible with County applications is at the risk of each Department).

c. Anti-virus Software

1. Standards

- a. Anti-virus signatures will be kept up to date.
- b. The client anti-virus agent will be configured to scan memory and drives.
- c. The client anti-virus agent will be configured to alert users a malicious activity is found.
- d. Log files on the client agent will be configured to be maintained for at least 30 days.

- e. Review of the anti-virus log is included in the incident response process.

2. Justification

In order for the County to be secure against viruses, every server and workstation needs to have anti-virus software installed and kept up-to-date. The chosen enterprise-level solution (read: centrally-managed) that has the capability to properly secure servers and workstations is approved but the responsibility of the Department. The Network Associates products are an industry standard.

3. Approved Solutions

Product	Version
VirusScan for Windows/Linux servers/workstations, or anything enterprise-level/centrally-managed (to allow for any products that provides similar protection.	Most recent available version with latest available virus definition update files (no later than one day); Windows servers must have an enterprise-level/centrally-managed AV product loaded

## 11. Mobile Devices

Note: Mobile devices are defined as any device that is used outside of a county network and not managed by vendor agnostic directory services term. This includes but is not limited to smartphones, PDAs, tablets (with or without cellular data plans).

a. User Mobile Device Standards

1. Minimum of 1-year manufacturer’s warranty.
2. Should have the latest version of the OS available for install on the device at the time of purchase.
3. Personal Mobile Devices are only allowed to connect to an ActiveSync compatible email server. All other access from the personal mobile device requires enrollment in the County/Department Mobile Device Management (MDM) system.
4. If a Mobile Device (Personal or County issued) is used for any access other than email, a County/Department approved MDM package is required. Any data storage on enrolled devices requires a solution as defined below.

5. Containerization - Gives the ability to securely deploy and manage county content in an encrypted space on the device. All resources, including proprietary applications and county email, calendar and contacts reside within this managed space. The password protected container gives users access to all county applications through authentication, providing a convenient way for users to access the managed space. The containerization approach allows IT to not only secure county data on a device, but also control which apps can access data and how that data is shared. If the data is compromised, the entire container or a specific application can be removed remotely without removing personal data from the device.
6. Secure Cloud – See Cloud Standards section.
7. VPN access is only allowed when delivered as part of the MDM delivered/managed solution.
8. Device inventory controlled within an MDM
9. Physical tracking: should be controlled by an MDM

b. Mobile Device Management (MDM) Standards

1. Supported platforms: Windows, iOS, Android ONLY
2. User authentication: MDM must be able to require users to authenticate.
3. Password policy enforcement: MDM must be capable of requiring a password – Proposed standard is a 4-character minimum password.
4. Remote lock/unlock of device: MDM must be able to remotely lock or unlock a device as needed by departments.
5. MDM must be able to report the following information of all devices connected through the MDM: device Serial Number, Phone number (if applicable), IMEI (if applicable), MDM should be able to provide GPS tracking/logging if desired by department.
6. Remote device wipe: MDM must be able to securely wipe all protected data from devices managed by the MDM.
7. Secure communication between MDM and device: All communication between MDM and managed devices must be secured by using HTTPS or more secure protocols.
8. The MDM must have the capability to push applications to managed devices.
9. The MDM should be capable to locking down non-compliant devices to prevent them from accessing County resources until the device is deemed compliant by the MDM rules set.
10. MDM should be able to control access to both websites and applications at department's discretion.
11. MDM must be able to initiate audits and report on compliance.
12. Data encryption enforcement of storage or external (SD card) storage: MDM must be able to enforce encryption of files on device, including but

not limited to internal storage and external attached storage (SD Card, USB, etc.).

13. Recommend: Remote control of device: This would help out in any troubleshooting of issues on end devices.
14. Recommend: Activity reports, web usage: MDM should be able to provide reports of web page usage if required by departments.

c. Approved Solutions

Mobile Devices

Supported Mobile Device platforms are Windows, Apple, Tizan (Samsung), and Android. Any Blackberry device currently supported will retain support until the device is end of life, but future purchases should not be Blackberry.

## 12. Development Tools

Note: Because a department's choice of development tools does not impact the County as a whole in the same way that their hardware and software platforms do, the following recommendations are guidelines rather than standards. However, departments choosing tools that are not on the following lists should be aware that:

- Information Technology Services (ITS) cannot guarantee support for these tools (e.g., ColdFusion, Macromedia's UltraDev) or for applications or Web pages built with those tools.
- Tools for developing Web pages that require server-side components other than ASP/ASP.NET (e.g., FrontPage extensions) may not be supported on the County's primary public Web server ([www.co.kern.ca.us](http://www.co.kern.ca.us))
- All Web development tools utilized for developing Web pages and Web applications must be consistent with and capable of meeting those goals identified in the "Recommended Guidelines/Minimum Standards for Kern County Web Pages" which may be modified from time to time by an affirmative vote of the Kern Information Technology User Group (KITUG).
- In cases where ITS is not using an item listed below, the department(s) currently using the tool will be listed as a potential resource for other departments considering the tool.

a. Standard

1. Report required ports and protocols needed to the ITS Network Administrator. The requested port and protocol will be reviewed and approved. If there is a request that is denied the Deputy CITO also needs to review the request.
2. Sensitive information, per the classification of data type, needs to be safe guarded. All encryption requirements will follow the Encryption standard requirements.
3. Remove any invalid URL or path references from the application.
4. The program will remove or disable unnecessary functionality.

5. Passwords built into the application will not display the account password as clear text.
6. The application will be able to handle the password complexity in the County Information Security Policy.
7. All accounts will be documented and maintained per the Information Security policy.
8. Application Development Methodology Documentation
  - Application Development Document
  - Business Scope
  - Data Requirements
  - Functional Requirements
  - Test Evaluation Report
  - Training Plan
  - User's Manual
  - Database Dictionary
  - Application Flow Chart
  - Application Wireframe

b. Justification

Development tools consist of applications that can be used for a variety of County services. Both the use and the type of development tool needs to be standardized to optimize operation and secure the application. Tracking changes and vulnerabilities can be maintained with a standard approach. If there is a business need to go outside of the standards, ensure ITS and the Deputy CITO are notified and approve the solution.

c. Approved Solutions

The versions of any software, tools, platforms or operating systems utilized with new development should be no more than two versions behind the current version. If there is a business need to operate at an older version level approval needs to be provided by the Deputy CITO. Prepare an approval letter to be signed including the business need, estimated time to upgrade, and number of versions behind.

d. Web Server and Application Server Operating System and Software

Note: The AS/400 is included as a Web server environment because it offers the ability to use existing hardware resources rather than maintaining a separate Web Server, and the ability to leverage existing skills of AS/400 programmers and developers. Although these reasons are sound, the AS/400 technology and personnel with these skill sets are phasing out and now most County Departments are using Microsoft IIS.

e. Recommendations

- Microsoft Internet Information Server (IIS), running on Microsoft Windows Server

- IBM's WebSphere Studio family (running in an AS/400 environment)
- Apache
- Tomcat

f. Library Management Software

- Microsoft Team Foundation Server
- SubVersion
- CVS; industry standard but not currently being used by the County

g. Databases

Environment Recommendation

For Web-based applications, the database should be located on a server separate from the Web server, unless the database activity is very limited, or unless a mid-range server like an AS/400 is being used as the Web server.

h. Product Recommendations

Category	Recommendation
Multi-user applications including existing or new client/server, Web-based or single-component database applications	<ul style="list-style-type: none"> <li>• Microsoft SQL Server</li> <li>• Oracle</li> <li>• SyBase</li> <li>• Informix</li> <li>• MySQL</li> <li>• PostGres</li> </ul>
Existing or new single-user applications	Microsoft Access
AS/400 applications	IBM DB2

i. Data-Mining/Reporting Tools

Product Recommendations

- Crystal Reports
- Microsoft SQL Server Reporting Services (SSRS)
- Monarch Pro
- Microsoft Business Intelligence
- Microsoft Analysis Services
- Microsoft Integration Services

j. Integrated Development Environment

Note: For the purposes of this document, an Integrated Development Environment is a programming environment that has been packaged as an application program, typically consisting of a code editor, a compiler, a debugger, and a graphical user interface (GUI) builder. Product Recommendations (for new development):

- Microsoft Visual Studio
- Jbuilder



- Eclipse
- IBM WebSphere Studio
- NetBeans

k. Programming Languages

Interpreted Programming Language / Development Tools Suite ASP/ASP.NET, JSP,  
 Compiled Programming Languages

- Visual Studio .NET
- ASP .NET
- Visual Basic
- Java
- C++
- C#

l. Scripting Language

- JavaScript or VBScript for server-side scripting; is browser-independent
- Php
- AJAX

m. Tag-based/markup-based Language

Note: for the purpose of this document, Cascading Style Sheets (CSS) will be included in this category.

- HTML
- HTML5
- XML
- CSS

n. Web Page Development Tools

1. HTML Editors

Because the choice of HTML editor is a personal preference, more than one HTML editor is recommended. An acceptable HTML editor should create non-browser-specific code (i.e. resulting HTML looks correct in Mozilla Firefox, Google Chrome, and Internet Explorer). Other recommended features are:

- Built-in code validation
- Preview option
- Color-coding or otherwise tagging various code components

Note: Software products that are not primarily HTML editors (e.g., MS Word, WordPerfect) should not be used to create HTML pages.

Recommended Product	Features/Comments
---------------------	-------------------

1 <sup>st</sup> Page	Free text-based editor with many of the same features as HomeSite.
DreamWeaver	Includes FTP/site management tools.
GoLive	Works seamlessly with Photoshop and other Adobe tools.
HomeSite	Extensive search/replace and validation functions.
HotDog	Text-based editor with preview option
TextPad	Text-based editor with compare feature, global search/replace, etc.
NotePad++	Text-based editor with color coding, line numbering and other advanced features.
IDE Based Editors	Embedded editors found in recommended IDEs with debugging support.

o. Image Creation and Editing Tools

As with HTML Editors, the choice of these tools is a matter of personal preference; therefore, more than one product is recommended.

- Adobe Photoshop, Illustrator
- Macromedia Fireworks
- Corel Graphics Suite (PhotoPaint, CorelDraw)
- Ulead PhotoImpact
- Paint
- InkScape
- Gimp

1. 3<sup>rd</sup> Party Add-Ins

- Telerik (toolkit)
- ComponentOne (toolkit)
- Net SQL Admin (security)
- Top Style (css)
- Fiddler (debugging)
- XAMARIN (phone)

## 13. Security Standards

Note: The following is meant for a generic approach to the County IT environment.

a. Auditing and Accountability

1. Standard

- a. Will comply with the Kern County Information Security Policy.
- b. Comply with all applicable federal, state, and county laws, regulations, and policies, in include records retention. Audit records

will include what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals associated with the event.

- c. Will ensure all backups performed on Kern County devices include audit logs on individuals accessing and changing logs.
- d. Will ensure permissions to audit logs is permitted to only administrators that have a need to know.
- e. All remote access to the Kern County network will collect VPN audit logs.
- f. Audit logs that are reviewed and found to have suspected violations will be reported to the Deputy CITO.

## 2. Justification

Audit logs generated by County devices ensure if an incident occurs the appropriate records of the incident are obtained. Audit logs provide accountability to County resources and access to County owned devices. All devices that are used to access County information need to be protected from unauthorized access to ensure the data is protected per County policies, State regulations, and any applicable laws. Ultimately the County is responsible for all data that is generated or stored on County assets.

## 3. Approved Solutions

The business nature of a County owned device is approved through the hardware County Standards. Auditing capabilities are managed through the device configuration and implementation of the device. For specific hardware refer to the Operating and System Standard.

## b. IT Contingency Planning

### 1. Standard

- a. Will comply with the Kern County Information Security Policy.
- b. Will identify all critical assets to the department and a method to continue operations when the asset is at a derogated or outage state.
- c. Will maintain an up to date list of all inventory and responsibilities parties to maintain the device.
- d. Will identify the department's recovery objectives and restoration priorities.
- e. Update the contingency plan when there are changes to the organization, information system, or environment of operation.
- f. Will maintain a current recall roster of needed personnel and vendors.
- g. Will conduct backups with off-site storage of essential assets to provide appropriate restore if needed.

- h. Will establish alternate communication channels in support of maintaining continuity of operations, at Department's discretion.

## 2. Justification

The County has a Contingency plan for all departments to be able to continue business operations. All IT contingency plans should be incorporated to the County priorities and business critical processes. The standards are to implement a required standard to prepare each department for continual business operations.

## 3. Approved Solutions

The business nature of each departments operation is the defined baseline.

## c. Physical Security

Note: If there is a business need to work on a computer device off site or at home all mobile devices need to abide by the standards of physical control. Mobile devices include any technology that can access County information and potential store County data.

### 1. Standard

- a. County owned devices that are used offsite or at home will have physical control over the device at all times.
- b. County owned devices that store sensitive information will provide appropriate encryption requirements per applicable federal, state, and county laws, regulations, and policies on hard drives, CDs, and USBs.
- c. Contain contact information if the device is lost and be reported to IT staff.
- d. Will comply with the Kern County Information Security Policy (Chapter 7).
- e. Will ensure when the device is being used to view sensitive information the device will not face others that are not authorized to see the information.
- f. County owned devices will only have authorized County employees, and/or County sanctioned personnel operate the devices (not to include public facing equipment).
- g. County owned devices where anti-virus software can be installed, will be in compliance with the anti-virus standards section.
- h. Personal devices used to access County information will not store or retain sensitive information on the device.

### 2. Justification

The purpose of physical security is to ensure all employees protect County information on devices that may not be located at a County building. All devices that are used to access County information need to be protected from unauthorized access to ensure the data is protected per County policies, State regulations, and any applicable laws. Ultimately the County is responsible for all data that is generated or stored on County assets.

### 3. Approved Solutions

For specific hardware refer to the County Standards workstation and mobile device sections.

#### d. Access Security

Note: The following is meant for a generic approach to the County IT environment. There are systems within the environment that will have separate requirements due to other applicable federal, state, and county laws, and regulations. Devices that fall into this category should be documented and approved by the County Deputy CITO or Department head. For devices that may not be able to meet the standards due to legacy equipment the devices should be documented and approved by the County Deputy CITO or Department head. All new purchased equipment should meet the standards stated below.

##### 1. Standard

- a. Will comply with the Kern County Information Security Policy.
- b. Will assign service accounts to systems for only needed interaction between the systems. Service Accounts are not to be used as administrative accounts.
- c. All enterprise admin, domain admin, and service accounts will be maintained in a password book. The password book will be provided to the department IT manager and locked in a secure cabinet.
- d. All account passwords will be treated as County sensitive information and safeguarded per Kern County Information Security Policy.
- e. All accounts associated to an administrator will be disabled within 24 hours of termination or leave of absence.
- f. Permissions provided to an account will be determined by valid access authorization, intended system usage, and attributes required by the departments business functions.
- g. Group accounts are not authorized unless the department head or designee has provided approval for business need.
- h. Accounts created will include a process to verify the user's identity for authentication.
- i. All administrative and user accounts to the Kern County network will enforce a limit of 5 consecutive invalid logon attempts will lock the account for a period of 10 minutes.

- j. Remote access to Kern County networks can be established through authorized VPNs or authorized email transmission.
- k. Only authorized County devices can be connected to the network.

## 2. Justification

Access to County devices and information needs to be controlled to ensure only authorized individuals can obtain County knowledge. All devices that are used to access County information need to be protected from unauthorized access to ensure the data is protected per County policies, State regulations, and any applicable laws. Ultimately the County is responsible for all data that is generated or stored on County assets.

## 3. Approved Solutions

The business nature of a County owned devices are approved through hardware Standards. Access control is managed through the device configuration and implementation of the device. For specific hardware refer to the County Standard workstation and mobile device.

### e. Reporting Phishing Attacks

#### 1. Standard

- a. All users that suspect an email to be phishing or malicious will send the email to the Department's local IT Help Desk. All users will wait further instruction from local IT Help Desk staff for the email. Users will not send the email to other staff member or to email distribution list.
- b. Local IT Help Desk will document the incident in the "Phishing Email Incident Report" and email to the [reportphishing@kerncounty.com](mailto:reportphishing@kerncounty.com) ITS Help Desk. The suspect email will be include with the report.
- c. The County Deputy CITO will review the suspect email and determine further mitigation steps. The report will be updated with the mitigation actions to take and send to all tenants.
- d. The tenant will have four hours to respond to the mitigation action to be completed. If there is a business impact from completing the mitigation action, the Phishing Wavier Request will be signed by the Department Head or designee with a description of impact. The wavier will be approved or denied by the County Deputy CITO.
- e. The County Deputy CITO and backup designee will have access to the all email tenants to perform periodic assessments of the mitigation actions. Any actions requested and not performed by the Department will be reported to the Department Head and Board of Supervisors as being non-compliant assessment finding. A report will be provided of the requests that were not completed.

#### 2. Justification

The purpose of standardizing the response to phishing attacks are to ensure all Departments are protected from potential harmful threats and minimize exposure. Emails are a high-risk point where any user can be taken advantage of and propagated throughout the environment. Phishing attacks are used as a launching point to harvest data or impact other business operations. Ensuring the reporting process is repeatable and measured for completion will further enhance the protected security controls.

### 3. Approved Solutions

For specific email services refer to the County Standards email section.

#### f. Multi-Factor Authentication

##### 1. Standard

- a. Register a device or alternative contact to register the authentication process, such as a cellphone, landline, or token device. A user when accessing the network will be challenged with the access code from the registered device.
- b. All lost or stolen devices will be reported to the IT Help Desk. The device will be removed from the system to ensure an access code is not sent to the device anymore.
- c. A user that fails the login after 5 times the account will lockout for 10 minutes.
- d. Conditional access will be configured to allow only authorized IP ranges and/or known locations.
- e. The Central Authentication Service (CAS) and Outlook Web Application (OWA) will have a trusted period up to 1 day.
- f. The Virtual Private Network (VPN) will require each session to require MFA.

##### 2. Justification

The purpose of multi-factor authentication is to enable a multiple layered method to access the County network. An access code is sent to the users registered device and the user has an account login to access the County network. Both layers must be used to access the network, which provides a strengthen security to County data and resources.

##### 3. Approved Solutions

Cloud solutions that access the County network; Office 365.

## 14. IT Media

### a. Social Media

#### 1. Standard

- a. Creation and ownership of County social media sites will be maintained by a County email address.
- b. Social media sites will not be maintained by personal emails or accounts.
- c. Passwords of a social media site will be identified as a service account and at a minimum will comply with section 704 of Chapter 7 Information Technology policy. Passwords will be kept in a password book and subjected to audits.
- d. Be identified as a sponsored County information site.
- e. Contain a link to the County’s Legal Disclaimer (<https://www.kerncounty.com/WebsiteUsagePolicy.aspx>)
- f. Contain contact information for the County program.
- g. Comply with all applicable federal, state, and county laws, regulations, and policies, in include records retention.
- h. Comply with section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), Subpart B, 1194.22.
- i. Will not contain posing support or opposition to, political campaigns, candidates, or ballot measures.
- j. Will not contain information that may compromise safety or security of the public or public systems.
- k. Will not contain content that violates a legal ownership interest of any other party.
- l. Will not disclose confidential or proprietary information.
- m. Will contain a disclaimer that if inappropriate information is posted on the site it will be removed.
- n. Will not disclose personal information about employees.  
Employees will identify themselves as County representatives.

2. Justification

The purpose utilizing Social Media is to increase the public’s knowledge, trust and use of County departments, programs, and services. Posts should always be related to work matters within the subject matter jurisdiction of the posting department and the County’s mission. The County Social Media sites or links must identify the department responsible for the information, such as descriptions, logos, and images.

3. Approved Social Media Sites

The following list has been vetted. If there are additional websites the department would like to utilize the department head or designee needs to provide additional approval and business needs.

<b>Approved Sites</b>
Facebook
Flickr



Twitter
UStream
YouTube
Linkedin
Instagram
NextDoor

## 15. Virtualization

This serves as guidance for the minimum standard requirements for Virtualization of Servers, Desktops and Applications, that may be installed or implemented within the Kern County Information Technology Infrastructure.

### a. Justifications

1. Migrating physical servers over to virtual machines and consolidating them onto far fewer physical servers, means reducing the overall footprint of your entire data center. Thus lowering monthly power and cooling costs in the data center.
2. Server virtualization enables elastic capacity to provide system provisioning and deployment at a moment's notice. An administrator can quickly clone a gold image, master template, or existing virtual machine to get a server up and running within minutes.
3. Virtualization allows an administrator to easily build out a self-contained lab or test environment, operating on its own isolated network.
4. Increase uptime, with capabilities such as live migration, storage migration, fault tolerance, high availability, and distributed resource scheduling.
5. Improve disaster recovery.
6. Isolate server applications; Server virtualization provides application isolation and removes application compatibility issues by consolidating many of these virtual machines across far fewer physical servers. This also cuts down on server waste by more fully utilizing the physical server resources and by provisioning virtual machines with the exact amount of CPU, memory, and storage resources that it needs.
7. Extend the life of older applications; by virtualizing and encapsulating the application and its environment, an administrator can extend its life, maintain uptime, and phase out legacy machines in the data center.

### b. Definitions

1. **Virtualization**, in computing, refers to the act of creating a virtual (rather than actual) version of something, including but not limited to a virtual computer hardware platform, operating system (OS), storage device, or computer network resources.

2. **Hardware virtualization** or platform **virtualization** refers to the creation of a virtual machine that acts like a real computer with an operating system. Software executed on these virtual machines is separated from the underlying **hardware** resources.
3. A **hypervisor** or virtual machine monitor (VMM) is a piece of computer software, firmware or hardware that creates and runs virtual machines. A computer on which a **hypervisor** is running one or more virtual machines is defined as a **host machine**. Each virtual machine is called a **guest machine**.
4. **Type 1** hypervisor runs directly on the hardware with virtual machine resources provided by the hypervisor.
5. **Type 2** hypervisor runs on a host operating system to provide virtualization services
6. **Snapshot** is a copy of the virtual machine's disk or file at a given point in time.
7. **Virtual desktop infrastructure (VDI)** is the practice of hosting a **desktop** operating system within a **virtual** machine (VM) running on a centralized server or a host.
8. **Application virtualization** is software technology that provides access to an application without being installed in the traditional sense, although it is still executed as if it were. The application behaves at runtime like it is directly interfacing with the original operating system and all the resources managed by it, but can be isolated or sandboxed to varying degrees.

c. Remote Display Protocol

Is a special set of data transfer rules that makes it possible for a desktop hosted at one place to display on a client's screen at another location.

d. Enterprise Virtualization Standards

1. Capable of taking a snapshot (or checkpoint, or point in time back-up)
2. Supports Virtual Networking
3. Capable of live migration of the VMs and or Applications
4. Enterprise level support Agreement is recommended
5. Can be used in redundant environment
6. Must comply with minimum County Network Connection and Security standards
7. Capable of dynamic resource allocation of a VM
8. Should support virtual guest / Application fault tolerance

e. Virtual Desktops

1. **Virtual Desktop Hosts:** Should comply with Enterprise Virtualization Standards.
2. **Bandwidth:** Appropriate bandwidth should be allocated, and a consistent, reliable network connection should be maintained.
3. **Security:** Must meet existing county security standards

f. Application Virtualization

1. **Remote:** An application is presented to the client from an external device or server where it's being executed, via a remote display protocol defined above.
2. **Streamed:** An application is transferred to the client from a remote device or server.
3. **Bandwidth:** Appropriate bandwidth should be allocated, and a consistent, reliable network connection should be maintained.
4. **Security:** Must meet existing county security standards

g. Application Hosting

1. **Virtual:** If an application is to be hosted in a virtual environment then the back-end servers must comply with Enterprise Virtualization Standards provided.
2. **Physical:** If an application is to be hosted in a non-virtual environment and the application is determined to be "Mission Critical" the application must be hosted in a clustered server environment

h. Approved Software Vendors

VMware – preferred

Microsoft Hyper-V

## 16. Cloud Standards

Note: To provide a standard that defines all Kern County information is protected and easily accessible when stored in a cloud service. Types of cloud service include the following:

- **Software-as-a-Service (SaaS)** is a cloud service model that one or more services (application or software) provided by a vendor, that runs at the vendor's data center (cloud environment) can be operated. The cloud environment offers reduced cost to the customer from not maintaining the hardware and software required to operate the service. Operating and securing the cloud environment is conducted by the vendor. The customer does not manage or maintain the underlying cloud infrastructure or any applications. Any administrative control over the application has to be negotiated with the provider. The data is typically owned by the customer and must be protected from other customer data and/or access.

- **Platform-as-a-Service (PaaS)** provides an environment for customers to create, host and deploy applications, saving developers from the complexities of the infrastructure side (setting up, configuring and managing elements such as servers and databases). PaaS can improve the speed of developing an app, and allow the customer to focus on the application itself. With PaaS, the customer manages applications and data, while the vendor manages operating system, virtualization, servers, storage and networking. The customer can choose to maintain the software or have the vendor maintain it. The cloud environment offers reduced cost to the customer from not maintaining the hardware and software required to operate the application/data storage. Security requirements are shared between both the customer and vendor of the cloud environment.
- **Infrastructure-as-a-Service (IaaS)** is a service that the basic computing infrastructure of servers, software, and network equipment is provided to the customer. The cloud environment offers reduced cost to the customer from not maintaining the hardware and software required to operate the computing environment. The customer has control over operating system(s), data storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). Security provisions are completely performed by the customer.

#### a. Deployment Models

1. **Private Cloud** is provisioned for exclusive use by a single organization comprising multiple customers. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
2. **Community Cloud** is provisioned for exclusive use by a specific community of customers from organizations that have shared concerns. It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and may exist on or off premises.
3. **Public Cloud** is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
4. **Hybrid Cloud** is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.

#### b. General Principles

1. The data generated by Kern County employees is the property of Kern County government. The electronic communications and records generated are “public records” under Government Code section 6253.9 (part of the Public Records Act) that provides essentially that even though records are in electronic format they are still subject to review and inspection by the public. To ensure all data can be collected for inspection the cloud service will need to provide this capability and maintain reasonable delivery time.

2. Kern County retains all personal property rights in any matter created, received or sent via the County's electronic communications systems and such matter is not the property of the employees or the provider housing the data in the cloud service. The contents of any electronic communications may be disclosed to authorized individuals within the organization without the permission of the sender, recipient, or creator of the communication. Employees or cloud provider should have no expectation of privacy in any matter created, received or send using the County's electronic communications system or cloud service. For cloud services that County staff do not have access to ensure appropriate measures are in place with the cloud provider to secure and provide communications when requested.

c. Cloud Service Standards

1. If a new cloud solution is desired, a Department will select a cloud service based on the Department(s) requirements. The Department will identify a reasonable justification to the County Deputy CITO. The County Deputy CITO has the right to deny the request with reasons and alternatives provided, wherein the Department can meet to develop a mutually agreeable solution.
2. Departments will provide a high level report of the new cloud solution before the new cloud service is procured and the report will be presented to the County Deputy CITO for review. Refer to Appendix A- Cloud Request for Services and Approval below for further information on the content of the report.
3. Identify with the cloud provider the mitigation in place to protect the robustness of privacy, confidentiality, integrity, and security controls.
4. Employees will comply with the Kern County Software Licensing and Use Policy, all software that is stored in the cloud still needs to be controlled through license agreements and copyright laws.
5. Department's will only procure cloud services that are currently listed in the Federal Risk and Authorization Management Program (FedRAMP) "Provisional Authorization" or "Authorization" listing. (NOTE: The FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring of cloud services.) The Department assumes risk if the vendor does not complete FedRAMP approval (fully authorized). If the vendor does not successfully complete the assessment, then the Department must migrate to another approved vendor.

6. Departments will develop a process with the cloud service provider to provide all data stored in the cloud environment to be identified for legal discovery by allowing all data to be located, preserved, collected, processed, reviewed, and produced.
7. Identify all data types and the required level of security requirements and reporting for the data type.
8. All data types identified will be secured per the security requirements mandated by data type. (i.e. Patient data will be protected under HIPAA guidelines. Personal Identifiable Information data will be protected under PII guidelines.) Employees will be familiar with any special requirements of access, protecting, and utilizing data, including Kern County Information Classification Policy and specific department sensitive data policy.
9. User awareness training will be provided to all employees dealing cloud storage and with the data types specific to the County department. The training will include the security measures to protect the different types of data in the department.
10. Employees will report all security incidents discovered in the cloud environment to their supervisor and Department IT. If there are signs the service in the cloud or a telecommunication device is compromised the Department's IT staff will ensure all usage of the service or device stops until the appropriate process has occurred to clean the infection or plug/contain the breach.
11. Employees will only access data in the cloud that has already been authorized through the supervisor and right-to-know/need-to-know. Users will be given access to data on a need to know basis.
12. Information that is accessed through the cloud needs to be transmitted through a secure communication transmission using FIPS140-2.
13. Business Associates with Kern County that may also need to access County data in the cloud environment will have appropriate non-disclosure agreements in place and given limited access through need-to-know.
14. The cloud environment will include the approved Kern County warning banner message (where possible). The warning banner will ensure all users are aware the site is monitored and could be subjected to forensic investigation.

d. Cloud Software-as-a-Service (SaaS) Standards

Note: Cloud Software-as-a-Service is defined as a software service that stores Sensitive County collected data and is stored in a contracted organizations location (other than Kern County network). The following can apply to other government agencies or commercial vendors. Software-as-a-Service may be a specific service residing on a Private, Community, Public, or Hybrid cloud, where the cloud infrastructure has not gone through the FedRAMP vetting process but is an industry accepted product.

1. A State or Federal agency (or organization contracted by the State or Federal government) SaaS system does not need to be approved by the County as those organizations hold and own data that Counties in California must provide and maintain for the State and Federal governments.
2. Data that does not contain sensitive data that is protected under laws and regulations the standards are recommended but not required. However, the data will be evaluated annually to identify if changes have been made to the data classification.
3. Software installed on County IT equipment will be inventoried to include the latest software version as soon as possible. The system will be updated with applicable patches as soon as the patch is tested. The software will be covered by maintenance agreements and updated if end of life.
4. Hardware devices supporting SaaS will be inventoried to include make and model. The hardware will be covered by maintenance agreements and updated if end of life.
5. Departments or County ITS (whomever contracts the service) will: Generate a data flow diagram will be prepared to include internal security controls between the outside organization and the county, data type, entry/exit points, and ports and protocols used.
6. Document ports and protocols used for the connection for the software-as-a-service and will include the port, protocol, service, purpose, and use.
7. Document access for all roles and permission levels. Access will be reviewed for users no longer requiring access to be removed from the system.
8. Monitor and disable inactive accounts after 90 days of non-use.
9. Grant access for need-to-know purposes to complete daily duties. And job functions.
10. Make sure the system will have at a minimum the County warning banner (if possible). If another government agency owns the system negotiate the appropriate warning banner to display.
11. Configure the software to have a session lock out after 15 minutes of idle time.

12. Users at a minimum will be required to provide username and password to authenticate to the software. There will be no group passwords unless it is for emergency access for the system administrators. The password requirement will at a minimum comply with Chapter 7 Information Security policy.
13. Wireless access will be documented and encrypted per FIPS 140-2 standards.
14. Public access will be documented and reviewed for business need. Sensitive data will not be displayed to the public until an appropriate public request form is completed and approved.
15. Users and administrators of the software-as-a-service will receive annual security training. Records of the training will be kept.
16. The software-as-a-service will audit successful and unsuccessful account logon events, account management events, and system events. For web applications all administrator activity authentication checks, authorization checks, data deletions, data access, data changes, and permission changes will be logged. Alerts should be configured for failed events.
17. Audit logs will be reviewed and if performed by the other organization shared with County IT administrators.
18. Audit logs will be stored for a year at a minimum.
19. Contingency planning for the service should be identified by the Service Provider per the departments needs and develop a backup strategy with the organization that can restore the data.
20. Sensitive data stored in the cloud-as-a-service will have encrypted data at rest implemented at FIPS 140-2 levels.
21. The data in transit (when the data is accessed and retrieved) will implement FIPS 140-2 levels.
22. Software solutions that meet the definitions of software-as-a-service that were in place before the cloud standards were added to the technology standards will be identified, assessed to the standards, and a plan put in place to meet the standard requirements by each department within 12 months.

e. **Standard Service Level Agreement (SLA):**

Departments will have SLAs with the Cloud vendor to include the following information at a minimum:

1. Clear definition of services and service levels.
2. Incident Reporting structure and process.
3. Agreed upon roles and responsibilities.
4. Disaster recovery.
5. Protection of sensitive Kern County data (for further reference of classification review Information Classification policy).
6. Performance measurement (such as response time resolution/mitigation time, availability, etc.).



7. Enforcement mechanisms to meet the service levels.
8. Conditions of termination and disposal or transfer of data.
9. Documentation of where data is physically stored.
10. Open to on-the-spot audits (where not covered by a higher governmental entity)

f. Justification

Cloud communication services provide a shared pool of configuration computing resources that can be procured for the County with minimal management effort or interaction. Kern County encourages the use of cloud services (SaaS, PaaS, and IaaS) when the interoperability, portability, security standards, bandwidth, and guidelines requirements are satisfied

g. Approved Cloud Solutions

The cloud solution has to possess approval through the FedRAMP process. If there are any solutions outside of this approval process the department should provide the completed Appendix A with the purchasing request. The purchasing request will be approved or disapproved by Risk Management, County Counsel, ITS and Deputy CITO to the Board of Supervisors. Risk Management will assess the cloud solution for cyber insurance coverage. County Counsel will assess the legal requirements and potential legal risk. The Deputy CITO will assess for potential security risk to data exposure.

The Board of Supervisors will have the final approval for the solution to be purchased and implemented. The Board of Supervisors will include the departments need to implement along with the purchasing approval.

h. Cloud Technology

1. Cloud communications services provide a shared pool of configuration computing resources that is stored outside of the County's IT network. Kern County encourages the use of cloud services once the interoperability, portability, security standards, and guideline requirements are satisfied. For specifics on the service requirements refer to the Information Technology Standards.
2. Cloud communication shall comply with current laws, regulations, and County policies.
3. New cloud solutions shall be approved by the Department Head, Risk Management, County Counsel, ITS and Deputy CITO to ensure the Kern County Technology standards and security measures have been met.

## Appendix A- Cloud Request for Services and Approval

Name of Requestor: _____	Email Address: _____
Primary Phone Number: _____	Alternate Phone Number: _____
Department Name: _____	
Alternate Name: _____	Email Address: _____
Primary Phone Number: _____	Alternate Phone Number: _____
Date of Request: _____	Need Date: _____

Check the following Cloud service being requested:

- Software as a Service - model that one or more services/applications are operated by vendor
- Platform as a Service - model on-demand services can be developed or deployed
- Infrastructure as a Service - basic computing environment maintained by vendor

Provide the mission need. *(Description of business needs to satisfy deficiency or enhance a capability.)*

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

What is the impact of not implementing the Cloud solution?

---

---

---

---

What type of department data is being stored in the Cloud?			
<input type="checkbox"/> Public Record	<input type="checkbox"/> PII-Personal Identification Information	<input type="checkbox"/> County Sensitive	
<input type="checkbox"/> HIPAA-Health Insurance Portability and Accountability Act			
<input type="checkbox"/> PCI-Payment Card Industry	<input type="checkbox"/> Other _____		

Is there a diagram of the design plan?  Yes  No Include with Form.

Is there a Contingency Plan in place?  Yes  No Include with Form.

Who will provide continuous monitoring services? \_\_\_\_\_

How does the service provider destroy the data stored in the Cloud? \_\_\_\_\_

Have all employees using County information been through training on how to handle data?  Yes  No

Has the service provider's solution been evaluated by Fed RAMP?  Yes  No

FedRAMP certification:  Authorized  Provisional Authorization

Is a Service Level Agreement (SLA) in place with the Cloud Provider?  Yes  No Include with Form.

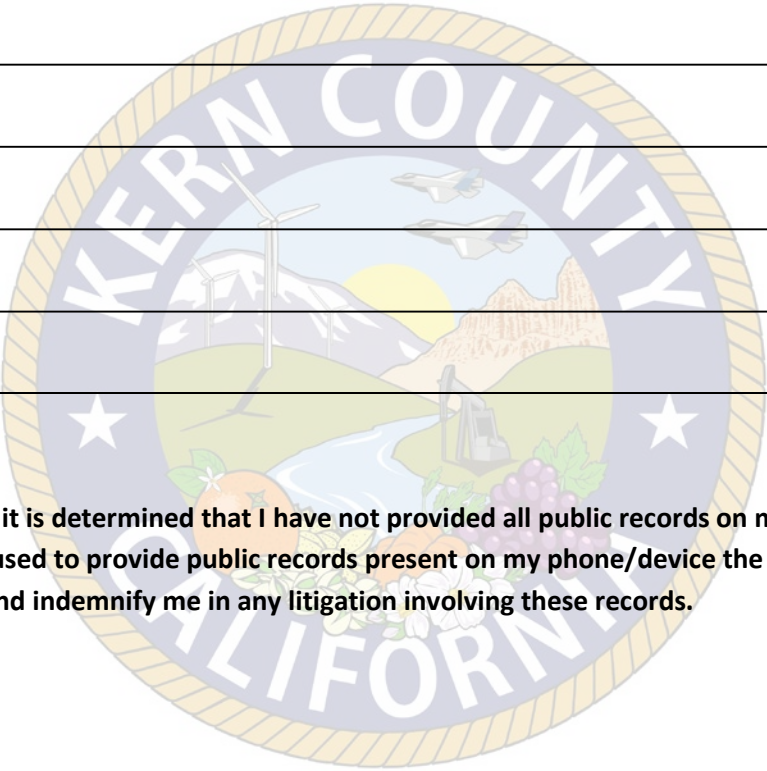
Does the SLA address the following?

- |  |  |
|--|--|
| Roles and Responsibilities                                   | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Incident Reporting Structure                                 | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Disaster Recovery  | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Availability of Service Thresholds                           | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Service Provider is aware of Data Type being stored in Cloud | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Performance Measures   | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Enforcement mechanisms to meet Service Levels                | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Termination and Disposal and/or Transfer of Data             | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Backup Strategy and Availability Thresholds                  | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Data Stored in the United States or its Territories          | <input type="checkbox"/> Yes <input type="checkbox"/> No |

# Employee Personal Communications Acknowledgment Form

**I certify that I have made a diligent search of my cell phone and/or personal device and that:**

- ┘ There are public records present on my cell phone/device that are responsive to the request and I agree to produce those records in a timely fashion.
  
- ┘ There are no public records present on my cell phone/device that are responsive to the request.
  
- ┘ There are records present on my cell phone/device that may possibly be responsive to the request and I decline to produce these records based on the following facts:



\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**I understand that if it is determined that I have not provided all public records on my phone/device and/or if I have refused to provide public records present on my phone/device the County may decline to defend and indemnify me in any litigation involving these records.**

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

## ARTIFICIAL INTELLIGENCE POLICY

1. *Purpose.* The purpose of this policy is to establish the guidelines and criteria used when determining if the use of generative artificial intelligence (AI) is acceptable and outline the acceptable uses of generative AI for Kern County employees. This policy is intended to ensure the risks of generative AI are understood to protect the safety, privacy, and intellectual property rights of the County of Kern.

2. *General Statement.* These policies and procedures adopted by the Board of Supervisors direct the delivery of technology services to departments, the use of the County's technology infrastructure by employees and the public and describes the information security practices that protect and secure Kern County's information and Information Technology (IT) resources, as required by California and federal law.

As generative AI technology advances, systems such as chatbots, virtual assistants, and other systems are becoming more prevalent and have the potential to serve as a value-added benefit to Kern County employees and for providing improved public services. These can include standalone systems, be integrated as features within search engines, or be overtly or transparently embedded in all manner of other software tools.

Generative AI tools have the potential to enhance productivity by assisting with tasks like drafting documents, editing text, generating ideas, and software coding. However, these technologies also come with potential risks that include data exposure, data exfiltration, inaccuracies, bias, manipulation, liability in the form of public records, and unauthorized use of intellectual property in the content generated. In addition, content created by AI, and the public availability of information submitted to the AI, could pose security or privacy concerns.

3. *Scope.* This policy is applicable to all employees of Kern County, including full-time, part-time, and temporary employees; contractors; students; interns; volunteers; and elected officials. The requirements defined in this policy are applicable to all communications, data, systems, and services owned and/or managed by Kern County; while in the performance of work-related functions, while on the job, or while using publicly owned or publicly provided information processing resources.

#### 4. *Definitions*

- a. **Generative Artificial Intelligence (AI):** For the purposes of this policy, generative artificial intelligence is the simulation of human intelligence processes, with machine learning models that result in capabilities such as generating text, images, or other media, using generative models. Generative AI models learn the patterns and structure of their input training data and then generate new data that has similar characteristics.
- b. **Machine Learning (ML):** For the purposes of this policy, machine learning is the development and use of statistical algorithms that can effectively generalize and thus perform tasks without explicit instructions.
- c. **Sensitive Data:** For the purposes of this policy, sensitive data includes any data governed by regulatory compliance, including but not limited to: Personally Identifiable Information (PII such

as social security number, full name, email address or any information that can be used to uncover an individual's identity), Personal Health Information (PHI, HIPAA, HITECH), Criminal Justice Information (CJI, DOJ, CJIS), or Payment Card Industry (PCI-DSS).

- d. Public AI: For the purposes of this policy, public AI refers to any cloud or vendor hosted AI system not owned and controlled by the County of Kern, including all forms of AI that do not meet the criteria of private AI.
- e. Private AI: For the purposes of this policy, private AI refers to an internally owned and controlled AI system, managed by County IT, reviewed and approved by the Chief Information Technology Officer and that reside within Kern County's infrastructure.

#### 5. *Criteria for Generative AI Use*

- a. The input provided to an AI system including sensitive data (PII, PHI, CJI, PCI, any regulated data) may not be used with public AI systems, unless that public AI system specifically meets the regulatory requirements of the data being provided.
- b. Where the output provided by public AI would present risk to the business if it were faulty or inaccurate, such as driving business process or supply chain activities, generative AI may not be used, unless such activity has been reviewed by and recommended by the Chief Information Technology Officer, and the Board of Supervisors has approved the specific risks as acceptable.
- c. Use of generative AI cannot be used in a mission critical capacity where loss of data or availability would impact business functions.

#### 6. *Generative AI Acceptable Use*

- a. Employees may use generative AI for approved business processes, such as research, data analysis, and communications, provided that organizational standards to protect data confidentiality and integrity, as laid out in this policy and elsewhere, are upheld.
- b. Employee use of generative AI systems must be lawful and not jeopardize the organization's professional reputation or brand.
- c. Employees will be accountable for any issues arising from their elective use of generative AI as part of business processes, including, but not limited to, copyright violations, sensitive data exposure, poor data quality, bias, or discrimination in outputs.
- d. Employees must not violate any privacy or data protection regulations when using generative AI systems.
- e. Privacy regulations and organizational processes designed to comply with them must be followed when entering data into the AI system, especially in cases involving a public AI system.

- f. AI-generated code must not be incorporated into any of Kern County's systems without appropriate code review and IT management approval.

7. *Enforcement.* Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

Department Heads or their designated representatives are responsible for disseminating and enforcing their employees' compliance with the provisions of this policy and for investigating non-compliance. When an instance of non-compliance with this policy is discovered or suspected, the agency shall proceed in accordance with departmental and Kern County personnel policies. Employee's privileges may be revoked when deemed necessary to maintain the operations and integrity of Kern County information systems. User access, accounts, passwords, software, and hardware may be withdrawn without notice if an employee is suspected of violating this policy. Employee discipline may be appropriate in cases of non-compliance with this policy. Criminal or civil action against employees may be appropriate where laws or rights are violated.

***Employees need to know that any electronic media communication may be considered a public record subject to disclosure under California law.***

8. *Written Acknowledgment.* Department Heads shall have all employees acknowledge in writing that they have received and read this policy. Such written acknowledgment shall be retained in department files. (Nevertheless, the failure to provide such written acknowledgment shall not in any way limit the County's ability to enforce this policy).

9. *Noncompliance.* Violations of this policy will be treated like other allegations of wrongdoing at Kern County and will be investigated per established procedures. Sanctions may include, but are not limited to, one or more of the following:

- Oral and/or written warning
- Probation, suspension, or termination of employment
- Legal action per applicable laws and contractual agreements

**ACKNOWLEDGEMENT OF ARTIFICIAL INTELLIGENCE POLICY**

**NOTICE TO EMPLOYEES**

I, the undersigned County employee, hereby acknowledge receipt of a copy of the County's Artificial Intelligence Policy, Exhibit D to Chapter 7 of the County Administrative Policy and Procedures Manual, on the date appearing next to my signature below.

Dated: \_\_\_\_\_

Signature: \_\_\_\_\_

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



## ELECTRONIC SIGNATURE USE POLICY

1. *Purpose.* The Electronic Signature Use Policy is to authorize the use of Electronic Signature to be used by Kern County Agencies and Departments. This Policy establishes when electronic signature technology may replace a hand-written signature, with the goal of encouraging the use of paperless, electronic documents whenever appropriate and legal. This Policy applies to all signatures used in processing various County documents and assumes the County signer has been given the authority to sign as determined by the Departments business process.

While the use of electronic signatures is suggested and encouraged, this Policy does not require any Department to use electronic signatures, nor can the County mandate that any third party signing a document use electronic signature.

2. *Definitions.*

**Digital Signature** is a specific signature technology implementation of electronic signature that uses cryptography to provide additional proof of the identity of a signer and integrity of a document. This cryptography uses Public Key Infrastructure (PKI) technology to issue digital certificates. PKI technology is accepted by the California Secretary of State for digital signatures created by a public entity.

**Electronic Signature**, or **eSignature**, means an electronic identifier, created by computer, attached, or affixed to or logically associated with an electronic record, executed, or adopted by a person with the intention of using it to have the same force and effect as the use of a manual signature.

**Permitted Transactions and Notices** means electronic transactions and notices for which the use of Electronic Signatures is not prohibited under applicable law.

**Proxy Signatures** are when Person-A authorizes Person-B to sign Person-A's signature on his/her behalf. (This is prohibited for eSignatures by this policy.)

**Record** is information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. Documents or forms are records.

**Signature**, for the purpose of this policy, includes the use of initials.

3. *Legality.* The legality and use of Electronic Signatures are governed by federal and state law. (See 15 U.S.C. §§ 7001, et seq. [U.S. Federal Electronic Signatures in Global and National Commerce Act]; California Government Code §16.5; California Civil Code §§ 1633.1, et seq.)

4. *Policy.* This Policy applies to documents requiring a signature of any person where the signature is intended to show authorship, approval, authorization, or certification, as allowed by law. It is the Policy of the County to encourage the use of electronic signatures in all internal and external activities, documents, and transactions where it is operationally feasible to do so, where existing technology permits, and where it is otherwise appropriate based on the Department's preferences. In such situations, affixing an electronic signature to the document in a manner consistent with this Policy shall satisfy the County's requirements for signatures.

5. *Agency / Department Discretion.* Each Department has discretion to decide whether to permit the use of electronic signatures. Departments should work with County Counsel to determine where applicable laws permit an electronic signature to be used. In addition, each Department that opts to use electronic signatures must adopt/amend their business practices to support the requirements of this Policy.

6. *Requirements of eSignature.* The use of electronic signatures is permitted and shall have the same force and effect as the use of a hard copy signature if all the following criteria are met:

- a. The electronic signature is capable of verification.
- b. The electronic signature is under the sole control of the person using it.
  - o Email notifications requesting electronic signatures must not be forwarded.
  - o These requirements prohibit the use of proxy signatures.
- c. The electronic signature is linked to the data in such a manner that if the data is changed after the electronic signature is affixed, the electronic signature is invalidated.

These requirements are facilitated by using the preferred eSignature Solution Providers as outlined in Section K of this Policy.

7. *Common Types of Documents.* This Policy is intended to broadly permit the use of electronic signatures. Examples of common types of documents are listed in the following table, with notes on each type of document. Departments should work with County Counsel to determine where applicable laws permit an electronic signature to be used.

<b>Document Type Examples</b>	<b>Is Use of an Electronic Signature Acceptable?</b>	<b>Notes</b>
Internal and External Memos and Forms	Yes	Electronic Signature is recommended.
Board Letters and Other Correspondence	Yes	Electronic Signature is recommended.
Contracts	Yes	Electronic Signature is recommended.
Certificates, Permits	Yes, if allowed by law	Departments should work with County Counsel to determine where applicable laws permit an electronic signature to be used.
Documents Requiring Notarization	No	
Documents Requiring the Board Chairman's Signature	Yes	Electronic Signature is recommended.

8. *Documents Involving Other Parties.* In the case of contracts or transactions which must be signed by outside parties, each party to the agreement must agree to the use of an electronic signature. No party to a contract or other document may be forced to accept an electronic signature. Other parties retain the right to revoke consent at any time, necessitating future documents to be signed in hardcopy format. When a document is electronically signed by all parties, the County will provide a copy of the electronically signed document to the other parties in an electronic format that is capable of being retained and printed by the other parties.

9. *Setup & Use.* To setup employees authorized to send out documents for eSignature, Department should contact Information Technology Services to establish a 'Department admin', allowing Departments to determine and control who can send out documents on behalf of that Department.

10. *Storage and Archiving of Electronically Signed Documents.* If a document exists only electronically, steps should be taken by each Department to ensure that a fixed version of the final document is stored in some manner. It is up to the Agency/Department to decide how to store these final electronic documents so long as it does so in a manner consistent with any applicable County document retention policies and any applicable laws.

11. *eSignature Solution Providers.* Kern County Information Technology Services department will be responsible to determine acceptable technologies and eSignature providers consistent with current state legal requirements and industry best practices to ensure the security and integrity of the data and the signature.

In 2021, the Information Technology Services department entered into an agreement with DocuSign© to provide electronic signature capabilities and services to Kern County. DocuSign© is on the Approved List of Digital Signature Certification Authorities certified by the California Secretary of State for use by public entities.

In 2022, the Information Technology Services department entered into an agreement with Adobe© for Adobe Acrobat, Creative Suite, and Sign to provide electronic signature capabilities and services to Kern County. Adobe© is on the Approved List of Digital Signature Certification Authorities certified by the California Secretary of State for use by public entities.