6.100 - Information Security Policy

Effective Date: 07/13/04

PURPOSE

To establish countywide Information Security programs, related responsibilities and provide the principles and foundation to manage Risk and maintain compliance with applicable laws, regulations and contractual obligations.

REFERENCE

July 13, 2004, Board Order No. 10 — Board of Supervisors — Information Technology and Security Policies

May 8, 2007, Board Order No. 26 — Board of Supervisors — Information Security Policies

Board of Supervisors Policy No. 6.101 — Use of County Information Assets (Acceptable Use Agreement), attached thereto

Board of Supervisors Policy No. 6.104 — Information Classification Policy

Board of Supervisors Policy No. 9.015 — County Policy of Equity

County Fiscal Manual

Comprehensive Computer Data Access and Fraud Act, California Penal Code Section 502

California Civil Code Section 1798.29

ISO/IEC 27000:2015 Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls

NISTIR 7298 "Glossary of Key Information Security Terms"; National Institute of Standards and Technology

NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations

NIST SP 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

November 7, 2018, Board Order No. 16

DEFINITIONS

All capitalized terms not defined in this policy have the same meaning as set forth in Board of Supervisors Policy No. 6.102 - Endpoint Security Policy and Board of Supervisors Policy No. 6.104 - Information Classification Policy.

Authentication: provision of assurance that a claimed characteristic of an entity is correct.

Authorization: access privileges granted to a user, program, or process or the act of granting those privileges.

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

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

County Department (Department): any County Department as designated by the Board of Supervisors and any County commission, board, or office that the CIO and the CISO, in consultation with County Counsel, mutually determine, in writing, at any time shall be included in the definition of "County Department"

Encryption: the process of changing plaintext into ciphertext for security or privacy.

Endpoint: a computer or other device connected to a computer Network. An Endpoint may offer information resources, services and applications to users or other Endpoints on the Network. Endpoints can include, but may not be limited to, desktop computers, laptop computers, Network servers, Portable Computing Devices (Android/iOS tablets and smart phones) and Internet of Things (IoT) devices.

Governance: actions an organization takes to ensure compliance with its Information Technology policies, standards and procedures with the goal of meeting business requirements.

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

Information Asset: without limitation, digital Information and any item that processes, stores or transmits digital information and supporting infrastructure that is owned, leased, managed, operated, or maintained by, or in the custody of, the County or non-County entities and used for County purposes.

Information Owner: official with statutory or operational authority for specified Information and responsibility for safeguarding its generation, classification, collection, processing, dissemination, and disposal.

Information Security: the protection of Information and Information Assets from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide Confidentiality, Integrity, and Availability.

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

Information Security Program: formal documents that provide an overview of the security requirements for countywide Information Security and describe the program management safeguards and common controls in place or those planned for meeting those requirements.

Information Steward: an agency official with statutory or operational authority for specified Information and responsibility for establishing the Safeguards for its generation, collection, processing, dissemination, and disposal.

Information System: a discrete set of Information Assets organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Information.

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

Integrity: the property whereby an entity has not been modified in an unauthorized manner.

Need to Know: a method of isolating Information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms 'Need-to-Know" and "least privilege" express the same idea. Need-to-Know is generally applied to people, while least privilege is generally applied to processes.

Portable Computing Device: any nonstationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, USB storage devices, video cameras, and pagers.

Redundancy: duplication or repetition of elements in electronic equipment to provide alternative functional channels in case of failure.

Resiliency: the ability to recover quickly from a hardware failure, power outage or other interruption.

Risk: a measure of the extent to which the County is threatened by a potential circumstance or event. Risk is typically a function of: (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence.

> Note: Information system-related security Risks are those Risks that arise from the loss of Confidentiality, Integrity, or Availability of Information or Information Systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation.

Risk Management: the process of managing Risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an information system, and includes: (1) the conduct of a Risk Assessment; (2) the implementation of a Risk Mitigation strategy; (3) employment of techniques and procedures for the continuous monitoring of the security state of the Information system; and (4) documenting the overall Risk Management program.

Risk Mitigation: prioritizing, evaluating, and implementing the appropriate Risk-reducing Safeguards and countermeasures recommended from the Risk Management process.

Safeguard: a mechanism (software, hardware, configuration, etc.) that protects something, such as information.

Technical Security: the protection of Information Systems against unauthorized access to or modification of Information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such Threats.

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

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

Workforce Member: employees, volunteers, and other persons whose conduct, in the performance of work for Los Angeles County, is under the direct control of Los Angeles County, whether or not they are paid by Los Angeles County. This includes, but may not be limited to, full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to the County.

POLICY

General:

Los Angeles County's Information Assets are valuable and essential to the continued operation of the County; therefore, the County's Information, and Information that has been entrusted to the County, must be protected in a manner commensurate with its sensitivity, value, and criticality. The Confidentiality, Integrity and Availability of the County's Information Assets shall be protected from unauthorized disclosure, modification, or destruction, and shall be safeguarded to the extent permitted by law.

Countywide Information Security policies establish the minimum expectations to which County Departments shall adhere. Each County Department may, at its discretion, establish supplemental policies, standards, and procedures based on unique requirements of the Department as long as they do not conflict or contradict with countywide policies.

Security Principles:

Los Angeles County (County) Information Security practices shall conform to the following principles:

- Accountability — Information Security accountability and responsibility shall be clearly defined as part of a security management structure and be acknowledged by management and staff.
- Risks — Risks to Information Assets and Information Systems shall be assessed periodically and continually managed as part of an Information Security Risk Management program to address Threats, Vulnerabilities and Risks.
- Awareness — All Workforce Members with access to Information Assets must be aware of the need for Information Security and trained in what they can do to enhance security in support of the business of the County.
- Cost Effective — Information Security Safeguards will be cost-effective and proportionate to the Risks facing the Information Asset.
- Ethical — Information Assets will be used and operated in accordance with the County's ethics Policies and practices.
- Defense-in-Depth — Information Security controls will be selected and architected with Defense-in-Depth in mind by layering controls to provide multiple layers of protection.
- Equitable — Information Security policies will be balanced with the rights of customers, users and third-parties and the needs of the County to achieve its goals.
- Governance — Information Security policies, standards, procedures and guidelines shall be developed and implemented based on industry recognized security standards and best practices. These policies, standards, procedures and guidelines will be periodically reviewed and corrective actions taken to remediate identified deficiencies.
- Integration — Information Security is an important element of sound business management and should be an integral part of the County's Information management.
- Minimize Complexity — Information Technology services and systems should be designed to minimize the number of technologies and reduce Information Technology complexity.
- Least Privileges — Workforce Members, systems and processes will be granted only those privileges necessary to perform assigned functions.
- Separation of Duties — Responsibilities and privileges will be divided to prevent a person or a small group of collaborating people from inappropriately controlling multiple key aspects of a process and causing harm or loss.
- Timeliness — Organizations should act in a timely, coordinated manner to prevent, detect and respond to breaches of, and Threats to Information Assets.

Information Security Governance:

The CISO shall establish and chair a Governance body as a sub-committee of the County's Information Technology Governance structure. The membership of this group shall consist of the CISO, Deputy CISOs, the Departmental Information Security Officer (DISO) or designee from each County Department, select representatives from Internal Services Department (ISD), Information Technology Services (ITS) Security Operations Division and any other appropriate individual as determined by the CISO.

The CISO will, with the membership, develop a charter by which this body will operate. Said charter will include, definition of mission and vision, scope and authority, roles and responsibilities, designation of workgroups and operating norms.

Privacy:

Non-public Information that is accessed using County Information Assets shall be used in accordance with County and Departmental policies, standards, and procedures. Such Information shall not be exposed and/or disclosed to unauthorized individuals.

Confidentiality:

Unless specifically authorized by designated Department management or Departmental Policy, sending, disseminating, or otherwise exposing and/or disclosing Non-public Information is strictly prohibited. This includes, without limitation, Information that is subject to HIPAA, the HITECH Act, or any other Confidentiality or privacy legislation.

Integrity:

County Workforce Members are responsible for maintaining the Integrity of information and other Information Assets. They shall not knowingly or through negligence cause such Information to be modified or corrupted in any way that compromises its accuracy.

Availability:

Departments will design Information Systems with sufficient Resiliency, Redundancy and Safeguards to ensure appropriate levels of Availability to meet business needs.

County Workforce Members will not engage in activities that result in lack of Availability of Information and other Information Assets.

Access Control:

Access Control mechanisms shall be in place to protect against unauthorized electronic and physical access, use, exposure, disclosure, modification, or destruction of County Information Assets.

Access Control mechanisms may include, without limitation, hardware, software, storage media, physical security, policies, standards and procedures.

Access privileges of all Workforce Members must be defined based on their officially assigned roles within the County and their Department.

Access to County Information Assets must be authorized by a designated owner of such Information Asset and must be limited on a Need-to-Know basis to a reasonably restricted number of people in accordance with County and Department policy. Department management shall establish a process that periodically reviews Workforce Member access to Information Assets in compliance with countywide policies, standards and procedures.

Unless specifically authorized by Department management or policy, access to, and use of, any County Information Assets and any related restricted work areas and facilities is governed by the principle of "Least Privilege."

Access to County Information Assets must be evaluated and terminated or disabled at the time a Workforce Member is transferred or their role or assignment is modified.

Access to all County Information Assets must be promptly terminated or disabled at the time a Workforce Member ceases to provide services to the County.

Authentication:

Access to every County Information System shall have an appropriate user Authentication mechanism based on the sensitivity and level of Risk associated with the information.

All County Information Systems containing Non-public Information shall require user Authentication before access is granted.

County Workforce Members shall be responsible for protecting their Authentication mechanism granted to them. Workforce Member shall not share their Authentication credentials and other Authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, ID cards/tokens, biometric logons, and smartcards). Workforce Members are accountable for all activities performed under their Authentication credentials unless an investigation proves that the Workforce Member did not violate policy at the time of the Incident requiring the investigation.

County Workforce Members shall not allow others to access a system while it is logged on under their Authentication credentials. The only exceptions permitted are when the system cannot be configured to enforce a log-in, or where the business needs of the County Department require an alternate login practice for specified functions. Such circumstances should be documented and approved by the Departmental Information Security Officer (DISO) or designee.

Passwords or single-factor Authentication, shall be changed periodically and use complexity in compliance with County password security standards.

All vendor-supplied default passwords must be changed before any Information Asset is used for County business Authentication.

Two-factor Authentication is required for remote access and system administrator access to servers unless otherwise stated in County Information Security technical and operational standards.

Separation of Duties:

Whenever a County Information Technology process involves Non-public Information, the system must include controls involving a separation of duties or other compensating Safeguards that ensure that no one individual has exclusive control over these types of information.

Identification:

Each Workforce Member entering restricted Information Technology areas shall wear a County issued identification badge so that both the picture and information on the badge are clearly visible.

Workforce Members and guests not issued an identification badge by the County, must be issued a "Visitor" identification badge prior to entering restricted Information Technology areas. Information Owners of restricted areas must develop procedures for such issuance. Departments must determine appropriate circumstances where such "Visitors" must be escorted while in restricted areas.

Disposition of Information Assets:

The Chief Information Security Officer, in cooperation with the DISOs, will develop, maintain and distribute appropriate procedures by which information, electronic or physical, can be rendered unreadable and/or unrecoverable.

Each Department is responsible for ensuring that all Information Assets are rendered unreadable and/or unrecoverable, prior to disposition or reissuance to another Workforce Member.

When using a certified vendor to render Information Assets unreadable and/or unrecoverable, Departments must ensure the vendor's contract clearly identifies a County authorized sanitization method and that the Department obtains a certificate attesting to wiping the data in accordance with County security policies and standards.

Information Security Awareness Training:

The Chief Information Security Officer, in cooperation with the DISOs, will establish and maintain a countywide Information Security awareness training program based on the County's information security policies.

County Departments may develop additional Information Security awareness training programs based on their specific needs, legal requirements and sensitivity of information.

Countywide Information Security awareness training shall begin with Workforce Member new hire orientation and shall be conducted annually throughout a Workforce Members term of employment.

Information Security awareness training shall be provided to Workforce Members as appropriate to their job function, duties, and responsibilities.

Each County Department shall ensure that its Workforce Members participate in the countywide Information Security awareness training program. Workforce Member participation in Information Security awareness training should be documented.

Physical Security of Information Assets:

Each County Department shall develop a plan describing how all County Information Assets will be protected from physical tampering, damage, theft, or unauthorized physical access.

County Information Assets containing Non-public Information located in unsecured areas shall be secured to prevent physical tampering, damage, theft, or unauthorized physical access.

Physical Information Assets owned by the County shall be marked with some form of identification that clearly indicates it is the property of the "County of Los Angeles", in compliance with the County Fiscal Manual.

Personally-Owned Endpoints and Portable Computing Devices:

County Workforce Members may be permitted to use personally-owned Endpoints and Portable Computing Devices. Each County Department will develop appropriate policies, standards and procedures for Authorization, use and management of personally-owned Endpoints and Portable Computing Devices.

County Department policies, standards and procedures shall include at a minimum, requirements for:

- Operating System software and application software is kept up-to-date (e.g., critical updates, security updates/patches, and service packs).
- Antivirus/Anti-malware software is installed and up-to-date.
- Full disk or volume Encryption if the Endpoint or Portable Computing Device stores County Non-public Information.
- Use of password protection.
- Compliance with all County Information Technology standards and procedures.

Use of personally owned Endpoints and/or Portable Computing Devices may result in such devices, or portion thereof, being subject to legal discovery and public disclosure.

Policy Non-Enforcement:

Non-enforcement of any requirement in this or any Information Security policy or standard does not constitute consent on the part of County management.

Periodic Review:

Information Security policies and standards are subject to continuous, systematic review and improvement and are reviewed at least tri-annually and updated to reflect changes in business objectives and/or the Risk environment.

Departments are expected to develop and adopt a periodic review process of departmental policies and standards.

Applicability:

All County Departments, Workforce Members and County Information Assets.

Compliance:

County Workforce Members who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County Workforce Members, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County Information Assets, and other actions as well as both civil and criminal penalties.

Policy Exceptions:

There are no exceptions to this policy.

RESPONSIBILITIES

County Departments:

The head of each County Department is responsible for ensuring Information Security for the Information Assets for which they serve as Information Owner. Management of each County Department is responsible for organizational adherence to County Information

Security policies, operational and technical standards and procedures, as well as any additional policies, standards, and procedures established by the County Department. They shall ensure that all County Workforce Members are made aware of those policies, standards, and procedures and that compliance is mandatory.

Chief Information Officer (CIO):

The Chief Information Officer (CIO) shall ensure proper Governance of the County's Information Assets through the development and oversight of the County's Information Technology Strategic Plan and the development of countywide Information Security policies, standards, and procedures. These County policies shall include, without limitation, the appropriate operation, maintenance, access, use, exposure, disclosure, and modification of County Information Assets. When approved, these policies shall be published and made available to all County Workforce Members to ensure their awareness and compliance.

Chief Information Security Officer (CISO):

The Chief Information Security Officer (CISO) shall report to the CIO or designee and is responsible for the countywide Information Security Program. The responsibilities of the CISO include, without limitation, the following:

- Developing and maintaining the countywide Information Security Strategic Plan and overall countywide Information Security Program.
- Providing County Information Security related technical, regulatory, and policy leadership.
- Facilitating the implementation of County Information Security policies.
- Facilitating the implementation of a countywide Information Security Risk Management framework and program.
- Coordinating County Information Security efforts across organizational boundaries.
- Establishing and maintaining a countywide information security awareness training program based on the County's information security policies.
- Directing the countywide Incident response program.

County Departmental Management:

County Department Management or their delegates who bear responsibility for the acquisition, development, and maintenance of County Information Assets are Information Owners of said Information Assets within the control of or under the management of the County Department. For each type of information or Information Asset, Information Owners must:

- Designate the relevant sensitivity classification.
- Designate the appropriate level of criticality.
- Define which Workforce Members will be granted access.
- Approve requests for various ways in which the information will be used.
- Ensure that all contracts with third-parties comply with appropriate Information Security policies.

County Department Information Technology Management/Departmental Chief Information Officer (DCIO):

The responsibilities of Information Technology management and the Departmental Chief Information Officer (DCIO) of each County Department include, without limitation, the following:

- Manage County Information Assets within the County Department.
- Notify the CISO when a change in DISO has occurred.
- Ensure the County Department adheres to countywide Information Security policies, standards, and procedures and any additional policies, standards, and procedures established by the County Department.
- Ensure that County Information Assets are implemented and configured to meet County Information Security, technical and operational standards and procedures.
- Serve as the designated Information Steward for all Information Assets within the purview of the County Department unless such Information Stewardship is shared with another County Department, entity or third-party. In this capacity, under the direction of Department Management, will:
    - Ensure that all Information Assets adhere to countywide Information Security policies, standards, and procedures.
    - Implement Access Control systems to prevent inappropriate disclosure.
    - Ensure backups of Information Assets so that critical information will not be lost.

- ◦ Implement, operate, and maintain the security measures.
- ◦ Ensure that County Information Assets are maintained at current critical security patch levels.

Departmental Information Security Officer (DISO):

The Departmental Information Security Officer (DISO) shall report to the highest level of Information Technology management or to executive management within the County Department. The responsibilities of the DISO include, without limitation, the following:

- Manage Information Security of County Information Assets within the County Department.
- Assist in the development of countywide Information Security policies, standards and procedures.
- Develop Department Information Security policies, standards, procedures and guidelines.
- Lead the Departmental Computer Incident response program.
- Ensure the County Department is regularly represented within County Information Security Governance and Incident Response teams.
- Report County Information Security Incidents as required by County policy.
- Provide insight and direction with information Security awareness content within the department.

Information Stewards other than Departmental Chief Information Officers (DCIO):

Under the direction of Information Owners, Information Stewards are responsible for safeguarding the Information Assets, including:

- ◦ Ensure that all Information Assets adhere to countywide Information Security policies, standards, and procedures.
- ◦ Implement Access Control systems to prevent inappropriate disclosure.
- ◦ Ensure backups of Information Assets so that critical Information will not be lost.
- ◦ Implement, operate, and maintain the security measures.
- ◦ Ensure that County Information Assets are maintained at current critical security patch levels.

County Workforce Members :

County Workforce Members are responsible for acknowledging and adhering to County Information Security policies, standards, and procedures. Without limitation, Workforce Members are responsible for the following:

- Protection of County Information Assets for which they are entrusted; accessing, using, exposing, disclosing, and modifying County Information Assets only as authorized; and accessing and using them for their intended purposes.
- Required to sign the Acceptable Use Agreement as a condition of being granted access to County Information Assets. The Acceptable Use Agreement is set forth in Board of Supervisors Policy No. 6.101 — Use of County Information Assets.

RESPONSIBLE DEPARTMENT

Chief Executive Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004	Sunset Date: July 13, 2008
Review Date: August 25, 2008	Sunset Date: July 13, 2012
Review Date: July 19, 2012	Sunset Date: January 13, 2013
Review Date: June 27, 2013	Sunset Date: September 30, 2013
Review Date: September 18, 2013	Sunset Date: January 30, 2014
Review Date: January 15, 2014	Sunset Date: February 28, 2014
Review Date: February 19, 2014	Sunset Date: March 19, 2014
Review Date: March 19, 2014	Sunset Date: December 31, 2014
Review Date: January 6, 2015	Sunset Date: December 31, 2018
Review Date: November 7, 2018	Sunset Date: December 31, 2021