	SAN BERNARDINO COUNTY **POLICY MANUAL**	**No. 09-06** **PAGE** 1 **OF** 8 **EFFECTIVE DATE** May 6, 2025
POLICY: COUNTYWIDE INFORMATION SECURITY PROGRAM		**APPROVED** DAWN ROWE Chair, Board of Supervisors

POLICY STATEMENT AND PURPOSE

The purpose of this Policy is to establish a Countywide Information Security Program (Program) to provide a baseline of information security and privacy principles to manage and safeguard the integrity of the San Bernardino County telecommunications and computing infrastructure. This Program also facilitates a continuous risk-based cybersecurity awareness training program, and maintains compliance with applicable data privacy laws (e.g., Health Insurance Portability and Accountability Act, Information Security Practices Act), regulations and contractual obligations.

DEPARTMENTS AFFECTED

Board of Supervisors, all County Agencies, Departments, Board-Governed Special Districts, and Board-Governed Entities.

REFERENCES

Agreement for Acceptable Use and Confidentiality of County Information Assets (Attachment)

DEFINITIONS

Acceptable Use Agreement: A document that a user must sign in order to be granted access to a County computing device, system, application, and the internet.

Access Control: A security technique that regulates who and/or what can view or use resources in a County computing environment.

Chief Information Officer (CIO): The senior executive responsible for overseeing the County's information technology (IT) systems and strategies.

Chief Information Security Officer (CISO): The County's senior level executive who oversees the County's information, cyber, and technology security (i.e., Countywide Information Security Program).

Confidential Information: Non-public Information that is designated in writing as confidential and falls within a recognized exemption to the San Bernardino County Sunshine Ordinance, County Code of Ordinances Section 19.0101, California Government Code 54950, and California Public Records Act (Government Code Section 7920.005). Confidential Information may include: legally protected information, such as personally identifiable information and protected health information under HIPAA and the HITECH Act.

Data: A subset of information that is a representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented in a display device.

Data Asset: Transmissible and storable documents, files, and other records and any Information Technology that processes, stores, or transmits such records and supporting infrastructure that is owned, leased, managed, operated, or maintained by, or in the custody and control of, the County or non-County entities and used for County purposes.

Data Asset Integrity: The accuracy, completeness, consistency, and validity of a Data Asset.

Data Asset Owner: County official with statutory or operational authority or responsibility for safeguarding, generating, classifying, collecting, processing, disseminating, and disposing of Data Assets.

Departmental Information Security Representative (DISR): This designation refers to a functional role rather than an official job title or position. In this capacity, the appointed personnel represent the

appointing department in security-related matters (e.g., cyber, information, physical) providing support, communication, coordination, and collaboration with the County CISO or designee. The DISR must report to the department's Information Technology Unit highest management level or department executive management.

Departmental Policy: A document with high level statements of intention and direction specifically formulated and approved by the department's management or designated committee as guidance for the respective departments' Workforce Members.

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

Health Insurance Portability and Accountability Act (HIPAA): Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

Health Information Technology for Economic and Clinical Health Act (HITECH Act): Health Information Technology for Economic and Clinical Health Act, Public Law 111-005.

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: any communication or representation of knowledge or understanding such as facts, Data, or opinions in any medium or form, including electronic, textual, numerical, graphical, cartographic, narrative, or audiovisual.

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 Security: The protection of Information Systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Information Security Awareness Training Program (SAT): This program is an important element of keeping County Workforce Members aware of cybersecurity and information security Threats and vulnerabilities. This training provides valuable principles and techniques to improve awareness of cyber activities such as ransomware, phishing, and human error which have proven to be an existential Threat to County business and services.

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 principles, safeguards, and common controls in-place or those planned for meeting those requirements.

Information System: The interrelated components of Information Technology and Data Assets that form the cyberinfrastructure used by the County to conduct all aspects of County operations.

Information Technology (IT): 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 Assets.

Information Technology Governance: The processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals.

Information Technology Integrity: The condition of IT wherein the operational and technical parameters are functioning within the prescribed limits, unimpaired and free from deliberate or inadvertent unauthorized manipulation.

Information Technology Strategic Plan: An organization's process of defining its strategy or direction, and making decisions on allocating its resources to attain strategic goals, and details the comprehensive technology-enabled business management processes for an organization.

Innovation and Technology Department (ITD): San Bernardino County's primary technology service provider entrusted with managing and safeguarding the County's enterprise mission-critical systems and infrastructure. Any services within the organization/enterprise that are essential to everyday business operations are "mission-critical" applications. Cloud-based applications are considered essential software, as well, that can be accessed, monitored, and maintained.

Least Privilege: This principle is a security architecture designed so each entity is granted the minimum system resources and authorizations the entity needs to perform its function.

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.

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. Information system-related security Risks are those Risks that arise from a breach of confidentiality or the loss of Data Asset Integrity, Information Systems 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, and other organizations.

Risk Assessment: The process of identifying the Risks to system security (e.g., business systems, applications including websites), and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.

Risk Management: The process of managing Risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the County 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 (e.g., software, hardware, and configuration) that protects something, such as Information.

Technology Asset: This is any item of value to our stakeholders, which can be tangible (e.g., hardware or software, computing platforms, network devices), or intangible (i.e., data or information).

Technology Asset Owner: County official with statutory or operational authority or responsibility for safeguarding, generating, classifying, collecting, processing, disseminating, and disposing of IT.

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.

Workforce Member: Employees, contractors, volunteers, and other persons performing work for or providing services to San Bernardino 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 AMPLIFICATION

General

The County's Information System is valuable and essential to the continued operation of the County. Therefore, the County's Information System must be protected in a manner commensurate with its sensitivity, value, and criticality to maintain Information Technology Integrity and Data Asset Integrity.

Countywide Information Security policies establish the minimum expectations to which County departments must adhere. Each County department may, at its discretion, establish supplemental policies, standard practices, and procedures based on unique requirements of the department, as long as the department's supplemental policies, standard practices, and procedures do not conflict with or contradict the Countywide policies.

Confidentiality

Unless specifically authorized by designated department management or Departmental Policy, sending, disseminating, or otherwise exposing and/or disclosing Confidential Information is strictly prohibited. Any release or disclosure of information under this policy will be in compliance with Section 14 of the County Policy Manual entitled, Release of Information, Privacy and Compliance.

Integrity

Workforce Members are responsible for maintaining Data Asset Integrity and Information Technology Integrity. Workforce Members must not knowingly cause, or through negligence allow, Data Assets or IT to be modified or corrupted in any way that compromises its accuracy or function.

Availability

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

Workforce Members will not engage in activities that result in a lack of availability of Information Technology and Data Assets.

Access Control

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

Access Control mechanisms may include, without limitation, hardware, software, storage media, physical security, policies, standard practices 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 Data Assets must be authorized by a designated Data Asset Owner and must be limited on a Need-to-Know basis to a reasonably restricted number of people in accordance with County and Departmental Policy. Department management must establish a process that periodically reviews Workforce Member access to Data Assets in compliance with Countywide policies, standard practices, and procedures.

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

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

Separation of Duties

Whenever a County IT process involves Confidential Information, the system must include controls involving a separation of duties or other compensating Safeguards that ensure that no single individual has exclusive control over Confidential Information.

Physical Access Identification

Each Workforce Member physically entering a County facility or building including restricted Information System areas must wear a County issued identification badge so that both the Workforce Member’s 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 physically entering restricted Information System areas. 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 Data Assets

The County CISO shall review and provide recommendations for the procedures by which Data Assets, whether digital or physical, can be rendered unreadable and/or unrecoverable.

Each department is responsible for ensuring that Data Assets contained on digital media is rendered unreadable and/or unrecoverable, prior to disposition, reassignment, or reissuance to another Workforce Member.

When using a certified vendor to render Data 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 Information Security Policies and standard practices.

Information Security Awareness Training

The County CISO, in collaboration with the County Administrative Office, Human Resources Department and County elected office when applicable, are responsible to maintain and grow a Countywide SAT commensurate with business and technology Risk consistent with the County's Information Security Policies.

County departments may develop additional SAT based on their specific needs, legal requirements, and sensitivity of information.

Countywide SAT must begin at the time of Workforce Member new hire orientation and must be conducted annually throughout a Workforce Member’s term of employment.

The SAT must be provided to Workforce Members as appropriate to their job function, duties, and responsibilities.

Each County department must ensure that its Workforce Members participate in the Countywide SAT. Workforce Member participation in the SAT should be documented and the record retained for a minimum of three (3) years.

Physical Security of Data Assets

Each County department must develop a plan describing how all County Data Assets controlled or accessed by the department will be protected from physical tampering, damage, theft, or unauthorized physical access.

County Data Assets containing Confidential Information located in unsecured areas must be secured to prevent physical tampering, damage, theft, or unauthorized physical access.

Physical Data Assets owned by the County must be marked with some form of identification that clearly indicates it is the property of the "San Bernardino County", in compliance with the County standard practices.

Periodic Review

Information Security standard practices 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 standard practices.

Compliance

Non-enforcement of any requirement in this or any Information Security Policy or standard practice does not constitute a waiver of the requirement by County management.

County Workforce Members who violate this policy may be subject to appropriate disciplinary action up to and including termination as well as available legal remedies. Non-County Workforce Members, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County Data Assets, and other actions as well as available legal remedies.

RESPONSIBILITIES

County Departments – Department Heads

Department Head is responsible for ensuring Information Security for the Information Systems and/or the components for which they serve as Data Asset Owner or Technology Owner. Management of each County department is responsible for organizational adherence to County Information Security Policies, operational and technical standard practices and procedures, as well as any additional policies, standard practices, and procedures established by the County department. Department Heads must ensure that all Workforce Members are made aware of those policies, standard practices, and procedures and that compliance is mandatory. County elected officials, such as the District Attorney, Sheriff/Coroner/Public Administrator, Assessor/Recorder/County Clerk, and Auditor-Controller/Treasurer/Tax Collector, serve functionally as Department Heads for their respective offices. Department Heads are encouraged to work with the CIO and CISO for support and assistance in meeting these requirements.

County Chief Information Officer (CIO)

The County CIO must ensure proper Governance of the County's Information Systems through the development and oversight of the County's Information Technology Strategic Plan and the

development of Countywide Information Security Policies, standard practices, and procedures. These County policies must include, without limitation, the appropriate operation, maintenance, access, use, exposure, disclosure, and modification of Information Systems. When approved, these policies must be published and made available to all Workforce Members to ensure their awareness and compliance.

County Chief Information Security Officer (CISO)

The County CISO must report to the County CIO and is responsible for the Program.
The CISO shall collaborate with the District Attorney, Sheriff/Coroner/Public Administrator, Assessor/Records/County Clerk, and Auditor-Controller/Treasurer/Tax Collector to advise on and address potential security exceptions and to ensure appropriate security measures consistent with the Countywide information security program.

The responsibilities of the County CISO include, without limitation, the following:

- Developing and maintaining the Countywide Information Security Strategic Plan and overall 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 [e.g., National Institute of Standards and Technology (NIST) Cybersecurity Framework, International Organization for Standardization (ISO) 27002] and program.
- Coordinating County Information Security efforts across organizational boundaries comprised of all County department management or their delegates.
- Establishing and maintaining a Countywide Information Security Awareness Training Program based on the County's Information Security Policies and associated Information Security and Risks.
- Directing the Countywide Incident response program.

County Departments – Executive Management / Information Technology Management

Department Heads or their delegates who bear responsibility for the acquisition, development, and maintenance of IT and Data Assets are Data Asset Owners and Technology Asset Owners within the control of or under the management of the County department. For each type of Data Asset and IT, Data Asset Owners/Technology Asset Owners must, without limitation:

- 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 Data Asset and/or Technology Asset will be used.
- Ensure that all contracts with third-parties comply with appropriate Information Security Policies.
- Manage County Data Assets and Technology Assets within the County department.
- Notify the County CISO when a change in DISR has occurred.
- Ensure the County department adheres to Countywide Information Security Policies, standard practices, and procedures; and any additional policies, standard practices, and procedures established by the County department.

- Ensure that County Data Assets and Technology Assets are implemented and configured to meet County Information Security, technical and operational procedures and practice.
- Department management will manage and provide direction to the DISR.

Departmental Information Security Representative (DISR)

The DISR must report to the highest level of IT management or to the department's Executive Management. The responsibilities of the DISR include, without limitation:

- Participate in the development of Countywide Information Security Policies, standard practice, and procedures.
- Participate in the development of department Information Security standard practice and procedures.
- Facilitate the Department Incident response program.
- Report Information Security Incidents as required by County policy.
- Coordinate the development and distribution of Information Security awareness content within the department.

Workforce Members

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

- Protection of County Data Assets and Technology Assets to which they are entrusted; accessing, using, exposing, disclosing, and modifying Data Assets only as authorized; and accessing and using Data Assets and Technology Assets for their intended purposes.
- Workforce Members may use County Information Assets for minimal personal use, provided that the use (i) is not prohibited by County and/or Departmental Policies; (ii) does not interfere with County operations or the Workforce Members performance; (iii) does not consume undue County Information Technology resources; and (iv) has the appearance of professionalism, even if it is not used in a public setting.
- Signing the Acceptable Use Agreement as a condition of being granted access to County Data Assets and Technology Assets.

LEAD DEPARTMENT
Innovation and Technology Department

APPROVAL HISTORY

Adopted September 9, 1985
Amended May 6, 2025 (Item No. XX)

REVIEW DATES
May 2030