5.3.20 Data Retention and Destruction

(a) Introduction and Overview

The purpose of this policy is to ensure that necessary records and documents are adequately protected and maintained. Records that have reached the records retention maximum lifespan or that are no longer deemed necessary by the California Department of Corrections and Rehabilitation (CDCR), California Correctional Health Care Services (CCHCS), and California Prison Industry Authority (CALPIA), hereinafter referred to as department, are to be destroyed at the proper time and in a secure manner, consistent with records management policies outlined by the Secretary of State's Office. The policy also describes the obligations of department employees to retain electronic and non-electronic documents and their proper disposal.

(b) Objectives

The objective of this policy is to establish the requirements for retaining or disposing of paper and electronic documents including but not limited to:

(1) E-mails, texts, chats, and instant messages.
(2) Video, audio, and image files.
(3) Word processing and spreadsheet files.
(4) Website activity and history.
(5) Information posted on social networking websites.
(6) Voice mails and video mail.
(7) Computer programming information, system and audit logs, configuration details.
(8) Physical paper documents, media and artifacts.

(c) Scope and Applicability

(1) The scope of this policy extends to all state information assets owned or operated by the department, as well as information assets owned and operated by third parties (if applicable) on behalf of the department.
(2) This policy applies to the department's Chief Information Officer (CIO) or designee, program management, Owners of Information Assets, Department Information Security Officers, Records Management Coordinators (RMC), Records Management Assistant Coordinators (RMAC), Technology Recovery Plan Coordinators, and Information Asset Custodians.

(d) Policy Directives

(1) Pursuant to California Government Code Sections 12270-12279, the department shall set records retention schedules to address legal, statutory, and compliance requirements as well as litigation needs, business processes, and data privacy concerns. Storage requirements shall be coordinated with the department RMC to ensure compliance with the State Records Management Act.
(2) The department shall:
   (A) Ensure that roles and responsibilities for the identification, classification, and life cycle management of all department data and information assets are defined, documented, and implemented.
   (B) Ensure that all department information assets, including information and information systems, are categorized according to their criticality to department in accordance with SAM 5305.5, as well as to their sensitivity and susceptibility to inadvertent damage, loss or exposure and corresponding impacts to department.
   (C) Ensure that methods to protect the confidentiality, integrity, and availability of department data and information assets according to their classification are defined, documented, and implemented.
   (D) Ensure that conditions for access to and use of department information assets for all personnel are defined and documented.
   (E) Ensure that all personnel with access to department data and information assets are trained regarding data access and handling according to their roles and responsibilities.
   (F) Ensure that department data and information assets are used solely for their intended purpose.
   (G) Ensure that department data and information assets are securely destroyed and disposed of once they are no longer required by the department.
   (H) Ensure regular backups shall be completed based on department back-up and retention policy.

(e) Data Retention Requirements

(1) Retention procedures shall specify:
   (A) Steps used to archive information and locations where this information is stored.

(B) The appropriate destruction of stored information, electronic or other format, after the identified retention period expires. Such steps shall adhere to the requirements outlined in this policy.
(C) Chain of custody and handling of stored information, electronic or other format, when under litigation.

(2) In certain instances, individual business units have unique record retention requirements outside of documented groups. These requirements shall be documented as part of internal processes and procedures and communicated to the Information Security Officer (ISO), RMC and RMAC. Such requirements may include contractual obligations with customers or business contacts or data retention requirements to maintain business operations. In some instances, departments may need to retain electronically stored information for a historical archive.

(3) During the appropriate retention period for electronic records, archived data shall be retrievable. Doing so requires the following protocols:
(A) As new software or hardware is implemented, appropriate department support staff shall ensure new systems and file formats can read legacy data. This may require that older data is converted to newer formats where possible.
(B) Data that is encrypted shall be retrievable. The department shall implement key management procedures to ensure encrypted data can be decrypted when needed.

(4) When establishing record retention periods, the department shall rely on (in order of precedence):
(A) Federal and state laws and statutes and regulations.
(B) State guidelines, recommendations, rules, and statutory requirements.
(C) Internal department requirements and policies.

(f) Audit Controls and Management

Documented procedures shall be in place for this policy and reviewed annually and updated as needed. Effective organizational management, audit controls, and employee practices include:

(1) Documented record retention schedules and archival information of the department.
(2) Procedures and anecdotal evidence of data migrations to manage electronic record compatibility with newer systems.
(3) Documented encryption and decryption strategies that allow for retrieval of archival electronic records.
(4) Employee procedures and documentation of records management and archival processes.
(5) Direct observation of archival records organization and storage.

(g) Expiration of Retention Period

Once a record or data has reached its designated retention period date, the Owner of Information Assets shall refer to the department Data Retention Schedule for appropriate action in accordance with the California State Records Management Act.

(h) Sanitization and Destruction

(1) When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store or transmit sensitive or confidential data shall be properly disposed of in accordance with measures established by SAM 5900 and 1600. (See NIST 800-88, Guidelines for Media Sanitization for further assistance.)
(A) Physical media (paper print-outs and other physical media) shall be disposed of by one of the following methods:
1. Shredded using department issued cross-cut shredders.
2. Placed in locked shredding bins for third party shredding to come on-site, retrieve bins and securely shred.
(B) Electronic/Magnetic media (hard drives, tape cartridges, CDs, printer ribbons, flash drives, printer and copier hard drives, smart devices, etc.) shall be disposed of by one of the following methods: (See NIST 800-88, Guidelines for Media Sanitization, Appendix A for further details.)
1. Clear – applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques.
2. Purge - applies physical or logical techniques that render Target Data recovery infeasible.
3. Destroy - renders Target Data recovery infeasible and results in the subsequent inability to use the media for storage of data.

(2) IT systems that have been used to process, store, or transmit sensitive or confidential information shall not be released from the department's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

(i) Suspension of Record Disposal in Event of Litigation Hold

Preservation of data is a response to issues involving litigation, legislation, and requests for data pursuant to public records requests. The department shall comply with multiple federal and state laws, legal proceedings, state regulations and standards for the proper preservation and delivery of relevant physical and electronically stored information (ESI) in a timely and reliable manner. Legal counsel shall take such steps as necessary to promptly inform all staff of any suspension in the further disposal of documents. Please refer to the department eDiscovery and Litigation Hold Policy for further details.

(j) Roles and Responsibilities

(1) Department Chief Information Officer (CIO) or Designee
   (A) The CIO or Designee owns this policy and is responsible for ensuring that all users of department information assets are aware of this policy and acknowledge their individual responsibilities.
   (B) The CIO or Designee is responsible for ensuring that this policy is reviewed annually and updated accordingly.
   (C) The CIO or Designee is required to audit and assess compliance with this policy at least once every two (2) years.

(2) Department Information Security Officer (ISO)
   (A) The ISO shall ensure processes exist for the secure destruction of paper and electronic records when no longer needed.
   (B) The ISO shall ensure specific retention requirements for sensitive or confidential data as defined by the Owners of Information Assets are adhered to.
   (C) The ISO shall ensure the safe and secure disposal of confidential data and information assets.
   (D) The ISO shall assist Owners of Information Assets and Information Asset Custodians in the identification of data security controls and processes.

(3) Department Owners of Information Assets and Program Management
   (A) Owners of Information Assets shall ensure that no document is retained for longer than is legally or contractually allowed.
   (B) Owners of Information Assets shall implement data retention and disposal guidelines limiting data storage and retention times in accordance with legal, regulatory, and business requirements.
   (C) Owners of Information Assets shall define and enforce data retention requirements.

(4) Department Information Asset Custodians
   (A) Information Asset Custodians shall assist Owners of Information Assets in identifying data retention security controls commensurate with the classification of the data.
   (B) Information Asset Custodians shall document, implement, monitor, and maintain data retention security protection controls as defined by Owners of Information Assets.
   (C) Information Asset Custodians shall develop and implement tools, technologies, processes, and procedures to support, monitor and maintain data retention security controls.

(5) Department Records Management Coordinator (RMC) and Records Management Assistant Coordinator (RMAC)
   (A) The RMC, pursuant to Gov. Code 12274, shall assist the RMACs, Owners and Custodians of Information Assets in establishing proper data retention periods.
   (B) The RMC shall assist in training identified RMACs and entity staff in records retention.
   (C) The RMACs shall ensure that required data retention periods are maintained and data beyond the lifecycle of established policy is properly disposed.

(k) Enforcement

(1) Non-compliance with this policy may result in disciplinary or adverse action as set forth in the Department Operations Manual, Chapter 3, Article 22.

(2) The department shall comply with the information security and privacy policies, standards and procedures issued by the California Department of Technology (CDT), Office of Information Security (OIS). In addition to compliance with the information security and privacy policies, standards, procedures, and filing requirements issued by the OIS, the department shall ensure compliance with all security and privacy laws, regulations, rules, and standards specific to and governing the administration of their programs. Program administrators shall work with their general counsel, Information Security Officer (ISO), and Privacy Program Officer or Coordinator to identify all security and privacy requirements applicable to their programs and ensure implementation of the requisite controls.

(3) The consequences of negligence and non-compliance with state laws and policies may include department and personal:
(A) Loss of delegated authorities.
(B) Negative audit findings.
(C) Monetary penalties.
(D) Legal actions.

(l) Auditing

(1) The department has the right to audit any activities related to the use of state information assets.
(2) CDT OIS and the department have the statutory right to audit department readiness to respond and recover from an incident.

(m) Reporting

Violations of this policy shall be reported to the department ISO.

(n) Security Variance Process

If compliance is not feasible, or if deviation from this policy is necessary to support a business function, the respective manager shall formally request a security variance as defined by the ISO.

(o) Authority

This policy complies with State of California Government Code Section 11549.3.

(p) Revisions

The CIO or designee shall ensure that the contents of this article are current and accurate.

References

- State Administrative Manual, Section 5305.5, Information Asset Management
- State Administrative Manual, Section 5310.4, Individual Access to Personal Information
- State Administrative Manual, Section 5310.6, Data Retention and Destruction
- State Administrative Manual, Section 5310.7, Security safeguards
- State Administrative Manual, Section 5340, Information Security Incident Management
- State Administrative Manual, Section 5340.1, Incident Response Training
- State Administrative Manual, Section 5340.2, Incident Response Testing
- State Administrative Manual, Section 5340.3, Incident Handling
- State Administrative Manual, Section 5340.4, Incident Reporting
- State Administrative Manual, Section 5350, Encryption
- State Administrative Manual, Section 5365, Physical access
- State Administrative Manual, Section 5365.1, Access Control for Output Devices
- State Administrative Manual, Section 5365.2, Media Protection
- State Administrative Manual, Section 5365.3, Media Disposal
- Federal Information Processing Standard, FIPS 199
- National Institute of Standards and Technology Special Publications 800-53, Access Control, AC-3, AC-4
- National Institute of Standards and Technology Special Publications 800-53, Audit and Accountability, AU-2, AU-3, AU-13
- National Institute of Standards and Technology Special Publications 800-53, Configuration Management, CM-8
- National Institute of Standards and Technology Special Publications 800-53, Media Protection, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7
- National Institute of Standards and Technology Special Publications 800-53, Physical and Environmental Protection, PE-5, PE-19, PE-20
- National Institute of Standards and Technology Special Publications 800-53, Planning, PL-4
- National Institute of Standards and Technology Special Publications 800-53, Program Management, PM-9
- National Institute of Standards and Technology Special Publications 800-53, Risk Assessment, RA-2, RA-3
- National Institute of Standards and Technology Special Publications 800-53, Security Assessment and Authorization, CA-7

- National Institute of Standards and Technology Special Publications 800-53, System and Communications Protection, SC-4, SC-8, SC-13, SC-17, SC-28
- National Institute of Standards and Technology Special Publications 800-53, System and Services Acquisition, SA-11
- National Institute of Standards and Technology Special Publications 800-53, System and Information Integrity, SI-12
- California Department of Corrections and Rehabilitation, Department Operations Manual Chapter 3, Article 22
- California Department of Corrections and Rehabilitation, Department Operations Manual Chapter 1, Article 23, Sections 14060.6.5, 14060.6.6
- California Department of Corrections and Rehabilitation, Department Operations Manual Chapter 4, Article 38, Section 47110.15
- California Government Code Section 11549.3

Revision History
Effective: 11/30/2022