5.3.22 eDiscovery and Litigation Hold

(a) Introduction and Overview

Preserving data is necessary in response to reasonably foreseeable litigation, subpoenas, or Public Records Act (PRA) requests, and may be required under applicable state and federal laws and regulations. Data may include both physical and electronically stored information (ESI). ESI is broadly defined as any information stored in an electronic medium, regardless of its manner of creation or use.

(b) Objectives

The objective of this policy is to establish California Department of Corrections and Rehabilitation (CDCR), California Correctional Health Care Services (CCHCS), and California Prison Industry Authority (CALPIA), hereinafter referred to as department, requirements for identification, preservation, capture, and delivery of relevant data in response to requests for information, audit, archive, and legal proceedings.

(c) Scope and Applicability

(1) The scope of this policy extends to all information assets owned or operated by the department, as well as information assets owned or operated by third parties (if applicable) on behalf of the department.

(2) This policy applies to the department's Chief Information Officer (CIO) or their designee, data owners, legal compliance staff, Agency and Department Information Security Officers, Privacy Officers, Privacy Program Coordinators, Records Management Coordinator (RMC), Records Management Assistant Coordinators (RMACs), Information Asset Custodians, and all users of department information systems.

(d) Policy Directives

The department shall:

(1) Preserve specific active and archived stored information and follow department data classification procedures when a litigation hold request is made.

(2) Provide a written litigation hold notice to all involved parties with clear instructions on what should be preserved and held.

(3) Ensure data and metadata are stored in a manner such that the data source is known and secured.

(4) Ensure necessary and appropriate record retention systems are created and maintained consistent with the records management policies outlined by the Secretary of State’s Office.

(5) Ensure proper controls for the preservation of data are implemented, including electronic communications which may reasonably be subject to legal proceedings.

(6) Establish a process for the intake and fulfillment of PRA requests.

(7) Establish standard protocols for the collection, analysis, and delivery of data including chain of custody, data integrity and auditability of records.

(8) Provide Records Retention and eDiscovery training to appropriate staff.

(9) Return or destroy all preserved or archived data to the affected individuals and resume the normal destruction schedule after the legal duty to preserve evidence ends.

(e) Electronically Stored Information Subject to Discovery

(1) ESI is any information stored in an electronic medium, regardless of its format, location, or medium. ESI is subject to discovery in civil litigation and may also be requested under the PRA. ESI includes, but is not limited to:

(A) E-mails, texts, chats, and instant messages.

(B) Video, audio, and image files.

(C) Word processing and spreadsheet files.

(D) Website activity and history.

(E) Information posted on social networking websites.

(F) Voice mails and video mail.

(G) Computer programming information, system and audit logs, configuration details.

(2) In the event of a litigation hold, this policy shall supersede requirements set forth in the Data Retention and Destruction Policy.

(f) 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 years.
(D) The CIO or designee is responsible for establishing eDiscovery teams in order to efficiently and properly coordinate the responses to PRA requests and information, audit, archive and legal proceedings.

(2) Department Information Security Officer (ISO)
(A) The ISO is responsible for the oversight of all department data preservation and compliance requirements and ensures that all applicable standards and guidelines are maintained and reviewed regularly.
(B) The ISO shall assist in the development of data preservation, planning, and production of entity data assets.
(C) The ISO shall assist the RMC, RMACs, Owners of Information Assets, and Information Asset Custodians with ensuring that data preservation, storage, integrity, and delivery meet the SAM 5310, 5310.5, 5310.6 and SAM 5305 requirements for security and privacy.

(3) Department Owners of Information Assets and Program Management
(A) Owners of Information Assets and program management supporting the department mission, state essential functions, or critical infrastructure shall participate in records retention processes, and ensure data is classified, labeled, and managed according to defined standards.
(B) Owners of Information Assets supporting the department mission, state essential functions, or critical infrastructure shall ensure that records management is incorporated into standard business operation practices.
(C) Owners of Information Assets shall ensure that all pertinent data that is required for the eDiscovery process is preserved and maintained according to the department's defined standards.

(4) Department Information Asset Custodians
(A) Information Asset Custodians shall only assist with authorized data collection and preservation requests.
(B) Information Asset Custodians shall ensure that the integrity of the data collection and preservation process is maintained and the request is fulfilled.
(C) Information Asset Custodians shall ensure the requested data is secure and available to the legal team as needed.

(5) Department Legal Counsel
(A) Legal Counsel shall provide the department eDiscovery designee a written notice to suspend routine or intentional purging of relevant data including overwriting, reusing, deleting, or any other destruction of electronic relevant information.
(B) Legal Counsel shall notify appropriate parties when the obligation to retain the preserved data ends.

(6) Department Records Management Coordinator (RMC) and Records Management Assistant Coordinator
(A) The RMC, pursuant to Gov. Code 12274, shall assist the RMACs, Owners, and Custodians of Information Assets in establishing appropriate 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.

(g) 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, 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.

(h) 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.

(i) Reporting
Violations of this policy shall be reported to the department ISO.

(j) 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.

(k) Authority
This policy complies with State of California Government Code Section 11549.3.

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

References

- Statewide Information Management Manual, Section 5305-A, Data Retention and Destruction
- State Administrative Manual, Section 5010, Maintenance Records
- State Administrative Manual, Section 1600, Records Management
- State Administrative Manual, Section 5310.6, Data Retention and Destruction
- 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
- California Department of Corrections and Rehabilitation, Department Operations Manual Chapter 1, Article 16, Sections 13040.7, 13040.7.1, 13040.7.2
- California Department of Corrections and Rehabilitation, Department Operations Manual Chapter 3, Article 22
- California Department of Corrections and Rehabilitation, Department Operations Manual Chapter 4, Article 36, Section 47090.10
- California Department of Corrections and Rehabilitation, Department Operations Manual Chapter 4, Article 38, Sections 47110.7, 47110.16
- California Department of Corrections and Rehabilitation, Department Operations Manual Chapter 4, Article 45, Section 49020.10.6
- California Government Code Section 6250
- California Government Code Section 11549.3

Revision History
Effective: 11/30/2022