5.3.15 Acceptable Use

(a) Introduction and Overview

(1) Information assets owned by the California Department of Corrections and Rehabilitation (CDCR), California Correctional Health Care Services (CCHCS), and California Prison Industry Authority (CALPIA) (including but not limited to department data and information, laptops, cell phones, and removable storage devices) are strategic assets intended for official business use, and are entrusted to State personnel in the performance of their job-related duties.

(2) Inappropriate use of CDCR, CCHCS, and CALPIA (hereinafter referred to as department) information assets could negatively affect the confidentiality, integrity, or availability of the information, information systems, or other information assets of the department and the State of California. Consequently, it is important for all users to access or use information assets in a responsible, ethical, and legal manner that safeguards department data and information.

(3) Additionally, the appropriate use of information assets benefits the State and the department by strengthening the protection of the department and its personnel and business partners from illegal or potentially damaging activities.

(b) Objectives

This policy defines and establishes the requirements for the appropriate use and safeguarding of department information assets.

(c) Ownership of Information

(1) Data and information in hard copy format and that which is electronically created, sent, received, processed, or stored on information assets owned, leased, administered, or otherwise under the custody and control of the department are the property of the State. Any information, not specifically identified as the property of other parties and that is transmitted, processed, or stored on the department's and business partner Information Technology facilities and resources (including e-mail, messages, and files) is considered the property of the department.

(2) Individual access and use of department information assets is neither personal nor private. As such, department management reserves the right to monitor and log all employee use of department information assets with or without advanced notice.

(d) Scope and Applicability

The scope of this policy extends to all information assets owned or operated by the department and to all personnel authorized to use these assets.

(e) Policy Directives

(1) The department shall ensure that users use and protect department information assets in accordance with this policy and applicable information security and privacy policies.

(2) Department Unacceptable Use

The department shall ensure that users do not:

(A) Use department information assets to engage in or solicit the performance of any activity that violates laws, regulations, rules, policies, standards, and other applicable requirements issued by the federal government, the State of California, and the department.

(B) Use department information assets for personal enjoyment, private gain or advantage, personal gain, political activity, unsolicited advertising, unauthorized fundraising, or an outside endeavor not related to State business.

(C) Engage in any activity that attempts to circumvent or alter the function of the department's security controls (e.g., spoofing email, anonymous proxies, or unauthorized encryption), or other activities that may degrade the performance of information resources, or may deprive an authorized user access to department assets.

(D) Share their work-related account(s), passwords, Personal Identification Numbers, security questions/answers, security tokens (e.g., smartcard, key fob), or similar information or devices used for authentication and authorization purposes.

(E) Use department information assets to send or arrange to send emails or intentionally access sites that contain pornographic, racist, or offensive material, chain letters or unauthorized mass mailings, and malicious code.

(F) Users shall not connect or otherwise attach unauthorized devices or equipment to the department network infrastructure.

(f) Roles and Responsibilities

(1) The department Chief Information Officer (CIO) or Designee:

(A) 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) Is responsible for ensuring that this policy is reviewed annually and updated accordingly.
(C) Is required to audit and assess compliance with this policy at least once every two years.

(2) Department Information Asset Users:
(A) Shall use and protect department information assets in accordance with this policy and applicable information security and privacy policies.
(B) Shall report any security concerns pertaining to department information asset security of which they become aware to the department Information Security Officer (ISO), designee, appropriate security staff or their immediate supervisor. Security concerns with information assets may include unexpected software or system behavior, which could result in unintentional disclosure of information or exposure to security threats.
(C) Shall report any suspected or actual activities or events indicating misuse or violation of this policy to the department ISO, designee, appropriate security staff or their immediate supervisor.
(D) Shall be aware of and adhere to all department information security and privacy policies.

(g) Enforcement

(1) Non-compliance with this policy may result in disciplinary or adverse action as set forth in 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 department ISO.

(k) Authority

This policy complies with 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, Information Security Program Management Standard
- State Administrative Manual, Section 5305.3, Information Security Roles and Responsibilities
- State Administrative Manual, Section 5320.4, Personnel Security
- 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 41, Section 48010.5

- California Government Code, Section 11549.3

Revision History
Effective: 03/2022