5.3.6 Information Security Policy Development and Maintenance

(a) Policy

(1) California Correctional Health Care Services (CCHCS) has adopted the following principles to govern information security policy development and maintenance.

(A) Risk will be identified, assessed, and managed
(B) Risk tolerance levels will be constantly recalibrated
(C) Accountability over assets will be established
(D) Least privilege principle will be used to determine the degree of access
(E) Incompatible responsibilities will be separated
(F) Information and system integrity, confidentiality and availability will be maintained
(G) Personal privacy will be addressed
(H) Ethical behavior will be practiced
(I) IT Systems will be compliant with all applicable legal, statutory, and regulatory requirements

(b) Purpose

(1) Information security policies express CCHCS management's requirements for appropriately protecting enterprise Information Technology (IT) assets. Information security policies are meant to address all applicable organizational, business, legal, and regulatory information security requirements that are necessary to help ensure the confidentiality, integrity, and availability of CCHCS's IT assets. The objective of this policy is to explain the process used to develop and maintain CCHCS information security policies.

(c) Applicability

(1) This policy applies to all CCHCS IT assets and/or anyone that accesses or uses any CCHCS IT asset.

(d) Responsibility

(1) All CCHCS Employees and Contractors are responsible for:

(A) Reviewing and understanding this policy as it relates to their job role and responsibilities
(B) Communicating any risks or issues associated with the effectiveness of this policy and/or its enforcement to the CCHCS Office of Information Security (OIS)
(C) Immediately reporting any known areas of non-compliance to the CCHCS OIS

(2) ISO is responsible for:

(A) Authoring and enforcing this CCHCS information security policy
(B) Developing a performance metric to help articulate the organizational value of this policy and its effectiveness
(C) Reporting policy performance metrics to the Chief Information Officer (CIO)
(D) Managing the annual enterprise information security policy update process and ensuring tasks are completed effectively and on time

(3) Organizational Unit Managers are responsible for:

(A) Reviewing and understanding this policy as it relates to the objectives and operations of their organizational unit
(B) Continually assessing the effectiveness of this policy as it relates to their organizational unit's objectives and operations and reporting any issues or risks to CCHCS's ISO
(C) Promoting policy awareness, understanding, and compliance within their organizational business unit
(D) Immediately reporting any known areas of non-compliance to the CCHCS OIS

(4) CIO is responsible for:

(A) Reviewing and approving this policy
(B) Promoting policy awareness, understanding, and compliance throughout the organization
(C) Ensuring necessary resources are provided to support policy development, implementation, and compliance efforts

(e) Procedure

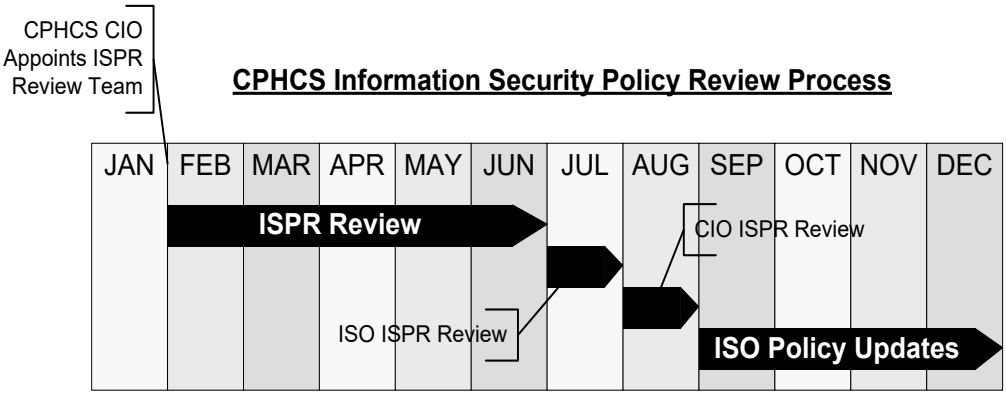
(1) Information Security Policy Development

(A) By the final business day of January each year, CCHCS CIO will appoint an Information Security Policy Review (ISPR) Committee. The ISPR Committee must include sufficient members to appropriately represent the enterprise in an effective and efficient manner. This committee will be accountable for representing and addressing information security policy development and maintenance activities. Each member will be

accountable for ensuring their organizational unit's information security policy requirements are addressed. CCHCS's ISO is responsible for managing the information security policy development process.

(2) Information Security Policy Review

(A) The appointed CCHCS ISPR Committee will meet regularly throughout the first half of the calendar year to assess the effectiveness and efficiency of existing information security policies, develop proposed changes to information security policies, and produce final proposed policy changes to the ISO by the final business day in June. The ISO will review all proposed policy changes and will produce a final set of recommended policy changes to the CIO by the final business day in July. The CIO will review the recommended policy changes and will provide his or her final approvals to the ISO by the final business day in August. The ISO will incorporate all approved policy changes into new policy versions and will manage the iterative release cycle. The iterative release cycle must ensure proper document versioning and change management procedures to capture any policy changes and provide a repository of previous versions. The iterative release process must also include updating any information security policy education and awareness components and effectively communicating any policy changes to the enterprise user population. This policy review cycle is outlined in the graphic below.



(3) Information Security Policy Implementation

(A) Authorized policy version updates will go into effect starting January 1st of each calendar year.

(4) Information Security Policy Awareness, Understanding, and Accountability

(A) All new CCHCS employees and contractors must sign an information security policy statement of compliance and accountability document before accessing any CCHCS IT assets. The statement of compliance and accountability document is meant to indicate that a signee: a) is aware of CCHCS's information security policies, b) understands how to comply with CCHCS's information security policies, and c) is accountable for ensuring compliance with CCHCS information security policies. In addition to the original signing of the statement of compliance and accountability, all CCHCS employees and contractors must resign the statement of compliance and accountability annually. Information security policies must be made available to any authorized requestor.

(5) Enforcement

(A) Violation of CCHCS's information security policies by an employee or contractor may result in immediate revocation of access rights to CCHCS's IT assets. Violations of security policies are subject to disciplinary action. The specific disciplinary action that shall be taken depends upon the nature of the violation and the impact of the violation on the CCHCS's IT assets and related facilities. A partial list of potential disciplinary actions follows:

1. Written reprimand
2. Suspension without pay
3. Reduction in pay
4. Demotion
5. Dismissal
6. Criminal prosecution (misdemeanor or felony, State or federal)

(B) CCHCS reserves the right to consider legal remedies, or prosecution, against any person or entity for violations of any law or regulatory compliance matter.

(f) Review and Approval

(1) This policy is approved by CCHCS's CIO and will remain authorized and enforceable until replaced by an updated policy version. This policy will be reviewed annually by CCHCS's ISO to ensure that it is current. Changes to this policy will only be applied by CCHCS's ISO. All CCHCS employees and contractors may submit suggested changes for the policy to the ISO in writing. Upon due consideration, the ISO may use the suggestions as part of the annual review and update of the policy. The primary dissemination vehicle for the CCHCS information security policies will be the CCHCS Intranet.

(g) Resources

(1) For questions or clarification please contact CCHCS OIS at CCHCS-ISO@cdcr.ca.gov.

Revision History
Effective: 01/2011
Revised: 03/07/2023