5.3.4 Digital Signature Security

(a) Policy

(1) Any use of digital signature technology within California Correctional Health Care Services (CCHCS) must comply with all requirements stated in the California Government Code Section 16.5 and California Code of Regulations, Title 2, Division 7, Chapter 10, Digital Signatures. This information can be reviewed at: https://www.sos.ca.gov/administration/regulations/current-regulations/technology/digital-signatures/government-code-16-5 and https://www.sos.ca.gov/administration/regulations/current-regulations/technology/digital-signatures.

(A) **Digital Signature Usage**

1. The use of a digital signature shall have the same force and effect as the use of a manual signature if and only if it embodies all of the following attributes:
   a. It is unique to the person using it.
   b. It is capable of verification.
   c. It is under the sole control of the person using it.
   d. It is linked to data in such a manner that if the data are changed, the digital signature is invalidated.

(B) **Authorized Digital Signature Solutions**

1. CCHCS authorizes the use of only Public Key Infrastructure (PKI) digital certificate based digital signature technology for the purposes of applying a digital signature to electronic forms or documents.

(C) **Approved PKI Solutions**

1. All PKIs that are used to produce digital certificates to create digital signatures for official CCHCS transactions must be approved by the California Secretary of State. The approved list of PKI vendors can be found at: https://www.sos.ca.gov/administration/regulations/current-regulations/technology/digital-signatures/approved-certification-authorities/.

(D) **Approved Digital Certificate Algorithms**

1. Digital certificates that are intended to apply digital signatures must comply with FIPS 186-2 standards. FIPS 186-2 requires that one of the following digital signature (ds) algorithms by employed: Digital Signature Algorithm (DSA), RSA (Rivest, Shamir and Adleman), or ECDSA (Elliptical Curse Digital Signature Algorithm).

(b) Purpose

(1) This policy is intended to detail the requirements for the developing and/or using digital signature technology with CCHCS systems and data.

(c) Applicability

(1) This policy applies to all CCHCS Information Technology (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) Complying with all policy provisions
(C) Communicating any risks or issues associated with the effectiveness of this policy and/or its enforcement to the CCHCS Office of Information Security (OIS)
(D) Immediately reporting any known areas of non-compliance to the CCHCS OIS

(2) Information Security Officer (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) CIOs are 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) Digital Certifcates

(A) Digital Certificate Storage: CCHCS requires that all digital certificates that will be used for digital signatures must be stored on a FIPS 140-2 certified Smart Card device. The Smart Card must also be configured to require a PIN to access the digital certificate stored on the Smart Card.
(B) Certificate Revocation Verification: Prior to applying a digital signature to an electronic document, the validity of the digital certificate used to apply the digital signature must be verified by performing a Certificate Revocation List (CRL) lookup.
(C) CRL Publishing: Any PKI deployed to support digital signature must update the associated CRL to an Internet accessible HTTP website at least once every 24 hours.
(D) Identity Proofing Requirements for Digital Certificate Requests: All CCHCS employees or contractors that require a digital certificate to apply a digital signature for CCHCS transactions must have their identity verified to ensure the requester is who he or she claims to be. CCHCS requires the verification process to include at least one in-person or face-to-face meeting whereby the requester presents an official U.S. Government, Military, or State identification card to a CCHCS agent authorized to verify identity prior to receiving the digital certificate. If electronic verification is used as part of the ID proofing process the requester must be assigned a unique username and must be challenged to provide knowledge of a secret password that is known only by the requester.

(2) Use and Application of Digital Signatures

(A) Authorized Users of Digital Signature
1. Only users formally authorized by CCHCS management to use digital signature technology can apply a digital signature to a CCHCS IT asset. Formal authorization can be achieved by completing a Digital Signature Request form, having it signed by designated CCHCS management, and having it stored on file for audit retrieval purposes. The Digital Signature Request form is available through CCHCS IT Division.

(B) Authorized Usage of Digital Signature
1. Digital signatures can only be used with those IT assets that have been formally authorized by CCHCS management for use with digital signature technology.

(C) Applying a Digital Signature
1. When applying a digital signature, controls must be in place to ensure user credentials are valid and verified. Controls must also be in place to ensure all communications between the application and the Smart Card containing the digital certificate are appropriate secured and encrypted.

(D) Lost or Stolen Smart Cards
1. All lost or stolen Smart Cards must be reported to the ISO immediately and no longer than 24 hours from the time it is recognized the Smart Card is missing.

(3) Enforcement, Auditing, and Reporting

(A) Violation of CCHCS's enterprise information security policies by an employee or contractor may result in immediate revocation of access rights to CCHCS's IT assets. Additionally 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 information and/or data 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 version. This policy will be reviewed annually by CCHCS's ISO to ensure that it stays 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. The ISO may use the suggestions as part of the annual policy review and update process. 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.

References

- California Government Code Section 16.5
- California Code of Regulations, Title 2, Division 7, Chapter 10, Digital Signatures

Revision History

Effective: 03/2011
Revised: 03/07/2023