AP 3721 Information Security

References:

Education Code Section 70902; 17 U.S.C. Section 101 et seq.;
Penal Code Section 502;
California Civil Code 1798.29, 1798.82, 1798.3, and 1798.84;
Family Education Rights and Privacy Act (FERPA);
California Constitution Article 1, Section 1;
Government Code Section 3543.1(b);
California Community Colleges Information Security Standard

1. DEFINITIONS. The following definitions shall apply to this procedure:

A. **Sensitive Data:** Information Classification that includes Personally Identifiable Information (PII), Protected Health Information (PHI), credit card information, and any data which is considered critical to the ongoing operations of Santa Clarita Community College District.

B. **Privileged Account:** An account that can take administrative action on Sensitive Data and services.

C. **Remote Access:** The ability to access a computer or a network, such as a District computer or network share, from a remote location. Remote access enables users to access the systems they need when they are not physically able to connect directly.

D. **Vulnerability:** Any hardware/software errors or other problems that could adversely affect the District.

2. Purpose and Scope

Local, state, and federal regulations mandate the protection of Sensitive Data for students, personnel, vendors, and others. The Santa Clarita Community College District ("District") takes the responsibility of protecting Sensitive Data seriously and recognizes that a robust security posture must be in place to protect the privacy and security of

Sensitive Data. The District is committed to protecting the Sensitive Data it collects, transmits, stores, processes, or archives.

In particular, Information Technology shall:

1. Develop and maintain an Information Security Program that outlines responsibilities all District employees or vendors must follow when accessing Sensitive Data.

2. Actively inventory, track, and remediate District devices that are connecting to internal network resources to ensure that only authorized devices gain access.

3. Work with District departments to ensure they have properly inventoried, classified and securely stored Sensitive Data in accordance with state and federal laws, industry best practices, and related Board Policies.

4. Conduct a risk assessment for each Information Technology system regularly, or when necessary due to a significant change to Information Technology systems. Document risks and associated security controls.

5. Actively manage, inventory, and track all authorized software running on District-owned systems. Prevent, to the best of our ability, unauthorized and malicious software from being installed or executed.

6. Configure and maintain network devices, end-user computing systems, and enterprise computer systems to operate securely, with proper authorization, authentication, and an auditable change management capability.

7. Continuously assess and remediate vulnerabilities including acquiring information on new vulnerabilities, periodic scanning, vulnerability assessment, and applying software updates and patches in a timely manner.

8. Ensure that internally developed software is designed with adequate security controls and properly tested prior to being placed into service. Internally developed software shall have an auditable change management process.

9. Third-party software or systems will be assessed regularly or as needed for adequate security controls prior to purchasing or renewing service contracts.

10. Provide a secure wireless environment to the internet for students, employees, and

guests. The wireless environment shall provide an auditable record of wireless usage.

11. Conduct regular backups and adhere to Information Security industry best practices to allow for recovery in the event of loss, corruption, or other similar event or circumstances that may occur.

12. Ensure the continued operation of the District's Information Technology systems following a man-made or natural disaster, including the creation, maintenance, and periodic testing of a District Business Continuity Plan and Disaster Recovery Plan.

13. Create and maintain a strong awareness of information security risks and mitigation techniques through increased awareness and training of its employees, students, and vendors to increase knowledge of their information security responsibilities and to minimize information security risks.

14. Ensure only authorized individuals access District resources through the implementation of information security controls.

15. Control, track, and audit the use of privileged accounts, restricting the use of these accounts to only users with a verifiable need as determined by their job assignment or supervisor. Provide an audit trail of changes made by privileged accounts to ensure only authorized changes are made by authorized users.

16. Control and monitor the information flowing through its network to detect and prevent data loss/exposure to unauthorized individuals.

17. Control access to information assets based upon the need to know. In particular, access to employee and student personal/financial information, health information, and credit/debit card payment information shall be closely controlled and monitored.

18. Provide for the timely creation and deactivation of accounts for students, employees, vendors, visitors, volunteers, and guests.

19. Ensure the proper protection of data, as defined in the Information Security Program, through access control and/or encryption while data is in transit through computer networks and while residing at rest on storage media on-site and off-site, on computer systems, and district mobile devices including laptops, tablets, and

mobile telephones.

20. Maintain the proper physical security mechanisms for the protection of information processing and storage facilities containing Sensitive Data, that are intended to protect such facilities from unauthorized access, damage, or interference.

21. Maintain accountability measures and security mechanisms at all times to control remote access to the District's systems and networks during external remote access use. External connections to the District's network must be established securely in order to preserve the integrity and availability of the network, including the integrity of data transmitted over the network.

22. Maintain incident response procedures, and respond to cyber-security incidents in a timely, thorough, and compliant manner.

23. Ensure that the District's cybersecurity capabilities are current and effective through periodic testing, audits, and internal and external reviews.

Reviewed and endorsed by CPC 4/27/21

Next review date: spring 2027