AP 3901 ELECTRONIC INFORMATION SECURITY

References:

BP 3720 Computer and Network Use
BP 5040 Student Records, Directory Information, and Student Privacy
BP 6960 Identify Theft Preventions
California Information Practices Act, Civil Code §§ 1798 *et. seq.*
Center for Internet Security Critical Security Controls (https://www.cisecurity.org/criticalcontrols.cfm)
Payment Card Industry Security Standards (https://www.pcisecuritystandards.org)

An essential purpose of this Procedure is to protect the confidentiality, integrity, and on-going accessibility of information stored, transmitted, and distributed electronically through the District's information technology systems, servers, and network.

In addition to this Procedure, colleges and departments are urged to establish best practices that reduce the collection, distribution, and retention of personal data, which are not necessary to perform the educational and business needs of the District.

Legal requirements and District Policy require that District personnel take appropriate measures to protect personal information, including employee and student records, from inadvertent or unlawful disclosure. Other legal requirements, such as is set forth in Civil Code § 1798.29, mandate that if certain personal information is inadvertently disclosed, the District/College must notify individuals whose information was compromised.

Detailed standards and practices associated with this Procedure reside in the current version of the District's Information Technology Security Standards and Protocols ("ITSSP") which is available at https://www.cccd.edu/itsecurity. The ITSSP describes in detail certain standards and practices, and best security best practices as outlined by the *Center for Internet Security Critical Security Controls* and *Payment Card Industry Security Standards,* and applicable state and federal law.

In particular, the District shall:

1. Actively inventory, track, and remediate devices that are connecting to its network to ensure that only authorized devices gain access.

2. Actively manage, inventory, and track all software running on District-owned systems allowing authorized software to be installed and executed and preventing unauthorized software from being installed and executed including, but not limited to, unlicensed software, malware, and associated computer viruses.

3. Configure and maintain its network devices, end user computing systems, and enterprise computer systems to operate in a secure manner, with proper authorization, and with an auditable change management capability.

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

5. Detect, and where possible prevent, the installation and execution of malicious code on the District's computer systems and network including the system-to-system propagation of this code.

6. Ensure that District developed software and software/systems acquired from a third party is developed with adequate security controls, properly tested, and remediated prior to being placed into service. District developed software shall have an auditable change management process.

7. Provide a secure wireless environment for students, employees, and guests supporting District-owned and personally-owned devices. The wireless environment shall provide an auditable record of wireless usage.

8. 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.

9. Create and maintain a strong awareness of IT Security risks and mitigation techniques through increased awareness and training of its employees, students, and vendors.

10. Ensure only authorized individuals access District resources through the implementation of appropriate standards on password length, complexity, history, and age.

11. Control, track, and audit the use of privileged accounts restricting the use of these accounts to only users with a verifiable need. Provide an audit trail of changes made by privileged accounts to ensure only authorized changes are made by authorized users.

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

13. Control access to the District's 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.

14. Provide the timely creation and deactivation of accounts for students, employees, vendors, visitors, volunteers, and guests in a manner commensurate with the level of access and permissions granted these individuals.

15. Ensure the proper protection of data through access control and encryption while data is in transit through computer networks, including email, and while residing on storage media on-site and off-site, on computer systems, and on mobile devices including laptops, tablets, mobile telephones.

16. Respond to cyber-security events in a timely, thorough, and compliant manner.

17. Ensure that its cyber security capabilities are current and effective through periodic testing, audits, and internal and external reviews.

Ratified October 18, 2016