Book	VCCCD Administrative Procedure Manual
Section	Chapter 3 General Institution
Title	AP 3721 INFORMATION SECURITY STANDARD
Number	AP 3721
Status	DRAFT
Legal	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
Adopted	TBD

Local, state, and federal regulations mandate the protection of the confidential information of students, faculty, staff and others. Ventura County Community College District has a high business dependency on this information, and a robust security posture must be in place to protect the confidentiality, integrity, and availability of this data. In keeping with its mission, the district is committed to protecting data it collects, stores, processes, or archives.

In particular, the District shall:

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

2. Properly inventory, classify and store sensitive or confidential data.

3. Conduct a risk assessment for each IT system on a recurring basis, or when necessary due to a significant change to information technology systems. Document risks and associated controls.

4. Actively manage, inventory, and track all authorized software running on district-owned systems. Prevent unauthorized and malicious software from being installed or executed.

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

6. 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.

7. Ensure that internally developed software and software/systems acquired from a third party are developed with adequate security controls and properly tested prior to being placed into service. Internally developed software shall have an auditable change management process.

8. Provide a secure wireless environment to the internet for students, employees, and guests. The wireless environment shall provide an auditable record of wireless usage.

9. 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.

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

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

12. 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.

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

14. 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.

15. 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.

16. 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.

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

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