# Chapter 3 – General Institution

## AP 3721 Information Security

**References:**

17 U.S.C. Section 101 et seq.; 42 U.S.C. § 1320d; 16 CFR Part 313; Penal Code Section 502(c) PC and 530.5 PC; California Civil Code 1798.29, 1798.82, and 1798.84; California Government Code §6250-§6270.5; Family Education Rights and Privacy Act (FERPA); ~~California Community Colleges Information Security Standard; California Community Colleges Data Security Standard;~~ NIST Special Publication 800-171 Revision ~~1~~ 3 **[Removed reference to the CCC Information Security Standard. Updated version of NIST 800-171 Rev. 3]**

Overview

This procedure will establish a framework to ensure confidentiality, integrity, and availability for the College's information systems. Under the direction of the College ~~President & CEO~~ **President/CEO**, the Chief Technology Officer or designee shall prepare and maintain a set of Information Security Standards based upon best practices that reduce the collection, distribution, and retention of personal data deemed unnecessary to perform the educational and business needs of the College. College personnel shall take appropriate measures to safeguard personally identifiable information, including, but not limited to, employee and student records, from inadvertent or unlawful disclosure. **[Updated President/CEO title.]**

Scope

The Information Security Standards apply to all facets of the College's data and systems, including, but not limited to, employees, students, contractors, vendors, service providers, volunteers, and other entities who come into contact with the College's data, whether in a paid or unpaid capacity. Exceptions to this shall be properly approved and documented by the Chief Technology Officer with direction from the College ~~President & CEO~~ **President/CEO**. **[Updated President/CEO title.]**

**Information Security Guidelines**

**Information security guidelines offer general instructions and recommendations of operations that provide a framework for achieving and maintaining compliance with information security standards. They are technical documents frequently updated to account for changes in College practices, application of technology, and use of data. These guidelines shall be developed and maintained by the College Information Technology department to document the proper use of its systems, processes, and data. [Sourced and reworded from College of the Canyons AP 3721.]**

**Controlled Unclassified Information**

**Employees may encounter or handle Controlled Unclassified Information (CUI) during their duties for the College. CUI encompasses unclassified information that must be protected or controlled in its dissemination according to legal, regulatory, or policy requirements. Despite not being classified, CUI is sensitive and significant, requiring**

measures to prevent unauthorized access. **[Sourced material from NIST 800-171 Revision 3 document. Defines Personally Identifiable Information (PII) as Controlled Unclassified Information (CUI).]**

Information Security Awareness Training

Employees are required to complete Information Security training. Training must be completed within 30 days of assignment and is mandatory upon hire and annually thereafter. This training is to communicate employee responsibilities when working with CUI as defined in AP 3721. The Information Security Awareness training program is subject to revision by the Chief Technology Officer or their designee. **[Keenan and Associates/SAFER cyber-liability insurance requirements for training and MFA.]**

Multi-Factor Authentication

Employees accessing Controlled Unclassified Information electronically will use a supported Multi-Factor Authentication medium. Multi-Factor Authentication controls are subject to revision by the Chief Technology Officer or their designee. **[Keenan and Associates/SAFER cyber-liability insurance requirements for training and MFA.]**

Information Security Standards

Information Security Standards are intended to protect and safeguard sensitive information entrusted to ~~Mt. San Antonio~~ the College to support its mission and educational goals. It is the responsibility of all users to ensure:

- Compliance with all applicable laws, regulations, and College policies and procedures governing information security and privacy.
- Confidentiality, integrity, and availability of sensitive data processed, stored, and managed by the College.

The College shall implement ~~the following~~ security standards to protect and safeguard its systems and data:

- ~~NIST Special Publication 800-171~~
  ~~The National Institute of Standards and Technology Special Publication 800-171 is based on the Federal Security Management Act of 2002 moderate level requirements. Through administration of financial aid via Title IV, Mt. San Antonio College is obligated to protect student information through controls outlined in NIST 800-171 to protect Controlled Unclassified Information (CUI): https://www.nist.gov/news-events/news/2018/06/nist-releases-update-special-publication-sp-800-171-revision-1-protecting~~
- ~~CCC Information Security Standard~~
  ~~The California Community Colleges Information Security Standard is a set of best information security practices created and maintained by the California Community Colleges System-wide Architecture Committee. Mt. San Antonio College's adoption of this standard supports the educational mission of the College by addressing the need to protect the confidentiality, integrity, and availability of its information systems and data: https://cccsecuritycenter.org/policy/policy-templates?download=70:ccc-information-security-standard~~

- ~~CCC Data Classification Standard~~

~~The California Community Colleges Data Classification Standard defines three levels of data classification and security levels placed on such data. Mt. San Antonio College's adoption of this standard supports the application of applicable security protocols to safeguard data collected and stored by the College:~~ ~~https://cccsecuritycenter.org/policy/policy-templates?download=69:ccc-data-classification-standard~~ **[Struck items due to outdated policies and broken web links. Section below with bullet points replaces this section.]**

- **Develop and maintain an Information Security Program that outlines responsibilities all College employees or vendors must follow when accessing College data.**

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

- **Manage network devices, user systems, and enterprise systems to ensure security, proper authorization, authentication, and a traceable change management process.**

- **Regularly evaluate and update the College's cybersecurity program through risk assessments, audits and reviews.**

- **Monitor and recommend remediation of system vulnerabilities by conducting assessments and promptly applying software updates and patches.**

- **Ensure that internally developed software incorporates robust security controls and undergoes thorough testing before deployment. Such software must also adhere to a documented and auditable change management process.**

- **Evaluate third-party software or systems for adequate security controls.**

- **Regularly perform backups for all critical systems to enable recovery in case of data loss, corruption, or similar incidents.**

- **Ensure the continuous operation of the College's Information Technology systems by creating, maintaining, and periodically testing the Crisis Management and Incident Response playbook.**

- **Maintain strong information security 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.**

- **Oversee, document, and audit the use of privileged accounts, ensuring these accounts are accessible only to users with a confirmed necessity established by their job role or supervisor.**

- **Maintain systems that provide timely creation, maintenance, and deactivation of accounts, access, and permissions for students, employees, vendors, visitors, volunteers, and guests.**

- **Ensure the proper protection of College data in transit through computer networks and while residing at rest.**

- **Ensure that all external connections to the College's network are established securely to protect the network's integrity and availability, as well as the integrity of data transmitted over the network.**

**[Section and bullet points above were sourced from College of the Canyons AP 3721 and modified internally to better reflect Mt. SAC needs.]**

Exceptions to Information Security Standards

Exceptions to information security standards shall be documented and recorded by the ~~campus~~ **College's** Information Technology department for approval by the Chief Technology Officer or their designee in consultation with the College ~~President & CEO~~ **President/CEO**. Requested exceptions must state a valid business justification and address the identified risk to the greatest extent possible afforded by the College. Accepted risks through the exemption approval process shall undergo annual review by the campus Information Technology department. **[Changed campus to College and updated President/CEO title.]**

Approved: January 8, 2020