Chapter 3 – General Institution

AP 3721 Information Security (NEW)

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

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 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.

Scope

The Information Security Standards applies 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.

Information Security Standards

Information Security Standards are intended to protect and safeguard sensitive information entrusted to Mt. San Antonio 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 standards:

- 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

Exceptions to Information Security Standards

Exceptions to information security standards shall be documented and recorded by the campus Information Technology department for approval by the Chief Technology Officer or their designee in consultation with the College 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.