This policy benefits entities by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity, and availability of data; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures and practices and know how to protect information.

It is the policy of SMC that the CIO selects from the NIST Cybersecurity Framework, controls, and enhancements along with procedures to implement these controls. These controls will promote and protect the integrity of information held by our organization. This policy has been approved by the Chief Information Officer on December 1, 2023.

This policy encompasses all systems, automated and manual, for which the departments and programs has administrative responsibility, including systems managed or hosted by third parties on behalf of those entities. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

The CIO is directed by this policy to implement controls and procedures that accomplish, wherever applicable, the following objectives:

- Defect remediation in information systems, software, and firmware updates, and incorporating these into our configuration management practices.
- Protection from malicious code.
- Monitoring of systems for signs of attack or unauthorized use of systems or information.
- Ensuring that our security and privacy functions are operating as expected.
- Verification of the integrity of firmware and software patches prior to their application.
- Protecting the organization from spam and spyware.
- Ensuring that College records are handled correctly through their life cycle.

a. Information security requires both an information risk management function and an information technology security function. Depending on the structure of the division, an individual or group can serve in both roles or a separate individual or group can be designated for each role. It is recommended that these functions be performed by a high-level executive or a group that includes high-level executives.

    1. Each division must designate an individual or group to be responsible for the ensuring that:

i. Risk-related

8. Determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data.
9. Participating in the response to security incidents.
10. Complying with applicable notification requirements in the event of a breach of private information.
11. Adhering to specific legal and regulatory requirements related to information security.
12. Communicating legal and regulatory requirements to the ISO/designated security representative, and
13. Communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.

1. Maintaining familiarity with business functions and requirements.
2. Maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security.
3. Assessing compliance with information security policies and legal and regulatory information security requirements.
4. Evaluating and understanding information security risks and how to appropriately manage those risks.
5. Representing and assuring security architecture considerations are addressed.
6. Advising on security issues related to procurement of products and services.
7. Escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures.
8. Disseminating threat information to appropriate parties.
9. Participating in the response to security incidents.
10. Participating in the development of enterprise policies and standards that considers the entity's needs, and
11. Promoting information security awareness.

8. Monitoring external sources for indications of data bư ẹſ

d. All information must be classified on an ongoing basis based on its confidentiality, integrity, and availability characteristics.

e. An information asset must be classified based on the highest level necessitated by its component data elements.

f. If the entity is unable to determine the confidentiality classification of information, or if the information is personally identifying information (PII) the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.

g. Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new confidentiality classification of the merged data is warranted. The merged data must be classified at least as high as the highest-classified component.

h. Full reproductions of information must carry the same confidentiality classification as the original. Partial reproductions may be evaluated to determine if a new confidentiality classification is warranted.

i. Each confidentiality classification has an approved set of baseline controls designed to protect these classifications and these controls must be followed.

j. SMC will communicate the requirements for secure handling of information to its workforce.

k. A written or electronic inventory of all information assets must be maintained.

l. Content made available to the public must be reviewed according to a process that will be defined and approved by SMC. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.

m. PII must not be made available without appropriate safeguards approved by SMC.

n. For non-public information to be released outside SMC, a process must be established that, at a minimum:

    1. Evaluates and documents the sensitivity of the information to be released or shared.

    2. Identifies the responsibilities of each party for protecting the information.

    3. Defines the minimum controls required to transmit and use the information.

    4. Records the measures that each party has in place to protect the information.

    5. Defines a method for compliance measurement.

    6. Provides a signoff procedure for each party to accept responsibilities, and

    7. Establishes a schedule and procedure for reviewing the controls.

Associated Standard: Account Management/Access Control Standard

a. Divisions must have an incident

b. Except as described in the Account Management/Access Control Standard, access to systems must be provided through the use of individually assigned unique identifiers, known as user-IDs.

c. Associated with each user-ID is an authentication token (e.g., password, key fob, multi-factor) which must be used to authenticate the identity of the person or system requesting access.

d. Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, clock) during the session lock.

e. Automated techniques and controls must be implemented to terminate a session after specific conditions are met as defined in the Account Management/Access Control Standard.

f. Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.

g. Tokens must not be stored on paper, or in an electronic file, hand-held device, or browser, unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the ISO/designated security representative.

h. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.).

i. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with entity missions and business functions (i.e., least privilege).

j. Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).

k. Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for business or other approved use consistent with policy, that user activities may be monitored, and the user should have no expectation of privacy.

l. Advance approval for any remote access connection must be provided by the entity. An assessment must be performed and documented to determine the scope and method of access, the technical and business risks involved and the contractual, process and technical controls required for such a connection to take place.

m. All remote connections must be made through managed points-of-entry reviewed by the ISO/designated security representative.

n. Working from a remote location must be authorized by management and practices which ensure the appropriate protection of data in remote environments must be shared with the individual prior to the individual being granted remote access.

Associated Standards: Account Management/Access Control Standard; Authentication Tokens Standard; Remote Access Standard; Security Logging Standard

a. Systems include but are not limited to servers, platforms, networks, communications, databases, and software applications.

    1. An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of the entity. A list of assigned individuals or groups must be centrally maintained.
    2. Security must be considered at system inception and documented as part of the decision to create or modify a system.
    3. All systems must be developed, maintained, and decommissioned in accordance with a secure system development lifecycle (SSDLC).
    4. Each system must have a set of controls commensurate with the confidentiality classification of any data that is stored on or passes through the system.
    5. All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources.
    6. Environments and test plans must be established to validate the system works as intended prior to deployment in production.
    7. Separation of environments (e.g., development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g., desktop background, labels).
    8. Formal change control procedures for all systems must be developed, implemented, and enforced. At a minimum, any change that may affect the production environment and/or production data must be included.

        a. Databases and Software (including in-house or third party developed and commercial off the shelf (COTS):
            1. All software written for or deployed on systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.
            2. Once test data is developed, it must ↳ centr to

8.]ήγᴰτɔᵐᵀ the

i. All security measures, including but not limited to access controls, system configurations and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed; or

ii. sensitive data is masked or overwritten with fictional information.

4. Where technically feasible, development software and tools must not be maintained on production systems by.

5. Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.

6. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.

7. Privileged access to production systems by development staff must be restricted. cocesses. ǩŌ

8. Deployment processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment. Separation of duties must be taken into consideration for these processes.

b. Network Systems:

do operation be infolimited be

limited is

that prod

6. Network authentication is required for all devices connecting to internal networks.
7. Only authorized individuals or business units may capture or monitor network traffic.
8. A risk assessment must be performed in consultation with the ISO/designated security representative before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

Associated Standards: Secure System Development Lifecycle Standard; Secure Coding Standard; Security Logging Standard; Secure Configuration Management Standard

a. Collaborative computing devices must:
    1. prohibit remote activation; and
    2. provide users physically present at the devices with an explicit indication of use.
b. Must provide simple methods to physically disconnect collaborative computing devices.

a. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.
b. All systems are subject to periodic penetration testing.
c. Penetration tests are required periodically for all critical environments/systems.
d. Where the entity has outsourced a system to another entity or a third party, vulnerability scanning/penetration testing must be coordinated.
e. Scanning/testing and mitigation must be included in third party agreements.
f. The output of the scans/penetration tests will be reviewed in a timely manner by the system owner. Copies of the scan report/penetration test must be shared with the ISO/designated security representative for evaluation of risk.
g. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions.
h. Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the ISO/designated security representative. The CISO must be notified in advance of any such tests. Any other attempts to perform such vulnerability scanning/penetration testing will be deemed an unauthorized access attempt.

i. Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested, and followed at all times to minimize the possibility of disruption.

Associated Standards: Patch Management Standard; Vulnerability Scanning Standard

a. All systems and the physical facilities in which they are stored must have documented operating instructions, management processes and formal incident management procedures related to information security matters which define roles and responsibilities of af

n. Audit logs recording exceptions and other security-relevant events must be produced, protected, and kept consistent with record retention schedules and requirements.

o. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound, and internal network traffic.

p. Monitoring systems must be configured to alert incident response personnel to indicators of compromise or potential compromise.

q. Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly.

    1. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers, and other communication equipment).

    2. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.

r. Backup copies of entity information, software, and system images must be taken regularly in accordance with the entity's defined requirements.

s. Backups and restoration must be tested regularly. Separation of duties must be applied to these functions.

t. Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.

Associated Standards: Secure Configuration Management Standard; Security Logging Standard; Cyber Incident Response Standard; Account Management/Access Control Standard

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.
If compliance with this standard is not feasible or technically possible, or if deviation from

Control	Actions taken or measures put in place to mitigate a risk.
Division	A unit of the college headed by a VP, Chief, Dean or Director
NIST	National Institute of Standards and Technology
Executive management	Senior Staff & President's Cabinet
Information Owners	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Defacements	Is an attack in which bad actors delete or modify the content on the SMC owned websites, replacing it with their own messages.
Visitors	Non-SMC Employees (Consultants & Contractors)

Submit all inquiries and requests for future enhancements to the policy owner at:

St. Mary's College
1928 St. Marys Rd.
Moraga, CA 94575

This standard shall be subject to periodic review to ensure relevancy.

1/23/2024	Publish	James Johnson
1/24/2024	Address GLBA Updates	James Johnson
2/7/2024	Shared With Provost Council	James Johnson

Lqnlu srio2
National Institute of Standards