Muskegon Community College

Information Security Policy

1. Purpose

Muskegon Community College (the College) shall develop, implement, and maintain a comprehensive Information Security Plan to help safeguard the confidentiality, integrity, and availability of campus information resources and address security requirements defined by Muskegon Community College policies, state and federal laws, and relevant contractual obligations.

2. Scope

This Policy is applicable to the College's employees, contractors, and third-party service providers.

3. Definitions

3.1. Information

Any entity or form that resolves uncertainty or provides an answer to a question or questions. A collection of data that imparts knowledge.

3.2. Information Systems

Collections of hardware, software, and services for collecting, processing, storing, and delivering information.

3.3. Information Security

The ongoing activities and processes for identifying, evaluating, and reducing risk to the College's information systems.

3.4. Information Asset

Any college-owned data, device, or other component of the environment that supports information-related activities.

3.5. Information Owner

An individual that utilizes an information asset to conduct the business of the College, with operational authority for specified information and responsible for authorizing the controls for generation, collection, processing, access, dissemination, and disposal of that information.

3.6. Information Custodian

The individual, team, or department responsible for the operation of an information resource. Individuals who obtain, access, or use information provided by Information Owners, for the purpose of performing tasks, also act as Custodians of the information and are responsible for maintaining the security of the information.

3.7. User

A person who interacts with information, other than an Information Owner or Information Custodian.

4. Roles and Responsibilities

All employees, contractors, and third-party vendors are responsible for supporting and complying with the requirements outlined in this policy. In addition, the following specific roles and responsibilities are identified in this policy:

4.1. ***Senior Management*** is responsible for:

- Final approval of Information Security Policy.
- Final approval of risk tolerance and risk acceptance.
- Allocating budget and resources for Information Security initiatives and oversight.
- Communicating and supporting Information Security awareness and compliance.

4.2. The ***MCC Data Integrity and Reporting Team*** is responsible for

- Reviewing and recommending strategies to implement the Information Security Policy (at least annually)
- Proposing risk tolerance and providing recommendations for accepting or rejecting risk related to security threats that impact the confidentiality, integrity and availability of Institutional Data.
- Identifying and documenting Information Owners.
- Identifying and documenting Information Custodians.

4.3. ***Information Owners*** are responsible for:

- Determining the appropriate criteria for obtaining access to College Information.
- Directing Information Custodians to grant and revoke access. Information Owners are accountable for who has access to their Information.
- Approving standards and procedures related to day-to-day administrative and operational management of Institutional Data.

4.4. ***Information Custodians*** are responsible for:

- Implementing appropriate physical and technical safeguards, to protect the confidentiality, integrity and availability of College Information.
- Granting and revoking access to College Information as authorized by Information Owners.

4.5. ***Users*** are responsible for:

- Adhering to policies, guidelines and procedures pertaining to the protection of College Information.
- Reporting actual or suspected vulnerabilities in the confidentiality, integrity or availability of Institutional Data to a manager or the Information Security Office.
- Reporting actual or suspected breaches in the confidentiality, integrity or availability of Institutional Data to the Information Security Office.

5. Information Security Principles

5.1. Least Privilege

The security principle that requires application of the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

5.2. Separation of Duties

Separation of duty, as a security principle, has as its primary objective the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific security process among multiple users and chains of command. Owners and custodians of information shall ensure the principle of "separation of duties" is enforced in security control (i.e., safeguards or countermeasures) and business operations.

5.3. Confidentiality

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]. A loss of confidentiality is the unauthorized disclosure of information.

5.4. Integrity

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]. A loss of integrity is the unauthorized modification or destruction of information.

5.5. Availability

"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]. A loss of availability is the disruption of access to or use of information or an information system.

6. Information Security Risk Management Framework

Muskegon Community College shall establish a framework for Information Security Risk Management. The framework shall consist of the following components:

6.1. An information security awareness program to inform College employees of policies, standards, and practices to prevent loss of Confidentiality, Integrity, or Availability;

6.2. Processes for the assessment and treatment of information security risk;

6.3. Policies and implementation standards that outline mandatory Information Security control categories, objectives, and requirements that must be achieved across the College;

6.4. A management process to oversee the performance and evaluate the effectiveness of the Information Security Program across the College at regular intervals.

7. Policy Objectives

7.1. Information Security Policy

This Information Security Policy defines Senior Management's objectives and support for Information Security. This Policy shall be:

- Reviewed by committee and approved by Senior Management;
- Published and communicated to employees and Third Parties; and
- Reviewed at least annually by Data Custodians and the MCC Data Integrity and Reporting Team. Reviews will occur more frequently if changes in Information Security threats and vulnerabilities require it.

7.2. Personnel Security

The College shall:

7.2.1. Ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions;

7.2.2. Ensure that College information and information systems are protected during and after personnel actions such as terminations and transfers; and

7.2.3. Shall employ formal sanctions for personnel failing to comply with information security policies and procedures.

7.3. Information Asset Management

Information Asset Management controls shall be implemented to identify, classify and assign responsibilities for protecting Information Assets, as practicable. Information Asset Management includes the following objectives:

7.3.1. Identifying and maintaining an inventory of Information Assets and the Information Owners and Custodians responsible for their protection;

7.3.2. Classifying Information Assets in a manner consistent with their value or business criticality; and

7.3.3. Defined acceptable use, management, transfer, storage and disposal practices associated with Information Assets in accordance with an information classification scheme.

7.4. Access Control

The College shall establish controls to limit information system access to authorized users and processes acting on behalf of authorized users. The College shall limit information system access to authorized devices (including other information systems) following the Principle of Least Privilege.

7.4.1. Local and remote access to College networks and information services shall be limited to authorized individuals with legitimate business needs.

7.4.2. Formal user provisioning and de-provisioning processes shall be implemented to ensure that creation of new accounts is authorized, users are uniquely identified, redundant user IDs are periodically removed, and that user IDs are disabled when no longer required.

7.4.3. Management of Privileged Access - Privileged access rights shall be appropriately evaluated, approved, periodically reviewed, and limited to only those users and applications with

legitimate and sufficient business need.

7.4.4. Passwords used to access College resources shall be established and managed in a formally approved and consistently secure manner.

7.4.5. Common secure logon practices shall be defined and implemented to ensure that means of access to College systems and applications effectively minimize the risks of unauthorized access threats.

7.4.6. Access to program source code for College systems shall be strictly controlled to authorized individuals only.

7.5. Cryptographic Security

The College shall:

7.5.1. Utilize cryptographic controls to address appreciable risks related to the confidentiality and integrity of sensitive information and non-repudiation of electronic transactions with College systems.

7.5.2. Generate, store, and manage cryptographic keys in a secure and approved manner.

7.6. Physical and Environmental Security

The College shall:

7.6.1. Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals;

7.6.2. Protect the physical plant and support infrastructure for information systems;

7.6.3. Provide supporting utilities for information systems;

7.6.4. Protect information systems against environmental hazards; and

7.6.5. Provide appropriate environmental controls in facilities containing information systems.

7.7. Operations Security

The College shall implement the following operations security controls:

7.7.1. Changes to business processes, information processes, facilities, and systems that may impact information security shall be appropriately identified, evaluated, communicated, and controlled.

7.7.2. The utilization of high value information resources shall be monitored, assessed, and optimized to maximize availability in conjunction with appropriate controls.

7.7.3. Detection, Prevention, and Recovery measures shall be established to protect College information systems against malicious software applications.

7.7.4. Development, testing, and operational environments shall be sufficiently separated and any sensitive information stored in these environments shall have at least equivalent protection measures.

7.7.5. Backup copies of valuable data shall be regularly created, stored securely, validated, and periodically tested for recoverability.

7.7.6. Important events related to College information assets shall be reliably archived, regularly reviewed, and protected from tampering and unauthorized access.

7.7.7. College information systems' clocks shall be synchronized against a single authorization reference time source.

7.7.8. Security weaknesses related to College information systems shall be promptly identified, assessed, and remediated according to the associated risks they present to the College.

7.7.9. Audit activities involving verification of production information systems shall be carefully planned, formally authorized, and executed by qualified personnel only.

7.8. Communications Security

The College shall implement the following communications security controls:

7.8.1. The management and provisioning of College network connections, services, and devices shall be limited to authorized personnel only.

7.8.2. Network traffic traversing College owned networks shall be filtered to address any appreciable risks and to preserve equitable availability of College network resources.

7.8.3. Network traffic traversing College owned networks shall be inspected for active attacks against College information assets. Interdiction capabilities shall be maintained to effectively block attacks that present appreciable risks to the College.

7.8.4. Network services, users, and information services shall be segregated on networks based on trust levels and associated risks.

7.8.5. Transfer methods and controls shall be defined and adhered to in order to protect College sensitive information traversing all forms of communication facilities to both internal and external senders and recipients.

7.8.6. Protection measures shall be established to safeguard College electronic messaging solutions from unauthorized access, modification or denial of service. Retention of electronic messaging communication shall be maintained in an approved manner.

7.8.7. Confidentiality agreements shall be used to establish legally enforceable terms of utilization and access for College confidential information for both external parties and employees.

7.9. Information Systems Acquisition, Development and Maintenance

The College shall implement the following security controls for acquisition, development, and maintenance of Information Systems:

7.9.1. The development and acquisition of information systems shall include the regular evaluation of security requirements in the earliest possible stages of related information system projects.

7.9.2. Secure program techniques and modeling methods shall be employed to ensure that coding practices adhere to best practices to limit potential for abuse.

7.9.3. Change control procedures shall be documented and enforced to ensure the confidentiality, integrity, and availability of information systems throughout maintenance efforts.

7.9.4. System acceptance testing shall include security testing and validation of effectiveness of controls related to any identified information security requirements.

7.9.5. If viable options are available, data that contains sensitive information shall not be used for system or application testing purposes. Test systems that do contain this data must adhere to common data security standards.

7.10. Third Party Access

Access to College information systems by third party vendors (i.e. contractors, partners, vendors, lessees) requires appropriate controls to protect College information assets. All third parties that have access to College information assets must comply with College information security policies and may be required to show proof of such compliance at any time.

7.10.1. Security requirements will be documented and agreed with each supplier that may access, process, store, or communicate College owned data.

7.10.2. Periodic review of supplier services will be conducted to ensure that related security agreements are being adhered to and enforced.

7.11. Information Security Incident Management

The following controls shall be implemented for Information Security Incident Management.

7.11.1. Information security events shall be reported through an approved channel and reviewed promptly by authorized Information Custodians.

7.11.2. Employees and contractors shall be encouraged to note and report any appreciable information security weaknesses observed in systems or services.

7.11.3. Response actions related to security incidents shall adhere to a documented set of procedures, including appropriate communication and coordination of efforts.

7.11.4. Knowledge gained during the analysis of security incidents shall be captured, reviewed, and appropriately shared to identify security corrections or control measures that may help address similar events.

7.11.5. Methods to preserve electronic evidence shall follow adequate standards of discovery and preservation to prevent spoliation.

7.12. Business Continuity Management

7.12.1. Planning shall be undertaken to ensure that appropriate levels of information security protection measures are maintained during emergencies or other adverse events. Periodic verification of these plans shall be performed on an annual basis.

7.12.2. Information processing facilities shall be implemented with redundancy sufficient to meet identified and documented availability needs.

7.13. Compliance and Audit

7.13.1. Regular periodic review shall be conducted to ensure that relevant policies, legal and contractual requirements are identified for the College and relevant information systems.

7.13.2. Procedures shall be implemented to ensure compliance with applicable legal, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products.

7.13.3. College records shall be protected from loss, destruction, falsification, and unauthorized release in accordance with legal, regulatory, and contractual business requirements.

7.13.4. The privacy and protection of personally identifiable information shall be ensured as required in relevant legal and regulatory frameworks.

7.14. Mobile Device and Teleworking Security

The College shall implement the following mobile device and teleworking controls:

7.14.1. Risks introduced by mobile devices shall be managed through mobile device policy.

7.14.2. Risks introduced by teleworking shall be managed through teleworking policy.

8. Policy Exceptions

Requests for exceptions to Information Security Policy shall follow controls for documenting the exception and associated risks with Senior Management approval. Exceptions shall be reviewed regularly by the MCC Data Integrity and Reporting Team.

9. Review

This policy shall be reviewed at least annually by the Data Integrity and Reporting Team, with recommendation to the Senior Management.

10. Compliance and Enforcement

Information Custodians are responsible for monitoring compliance with this policy and reporting instances of non-compliance to the Director of Compliance.

Effective Dates

This policy was approved by Senior Management on May 2, 2018, and is effective until May 2, 2019.