Southwestern Michigan College
Electronic Communication Policy

1.0 Purpose

The purpose of this policy is to formalize Southwestern Michigan College (SMC) access to systems and applications critical to maintaining the integrity of technology, data, and information and preventing unauthorized access to such resources. Access to SMC systems will be restricted to only authorized users or processes, based on the principles of need to know and least privilege, for all electronic communications equipment.

This policy will ensure College electronic resources are used for purposes appropriate to the College's mission. In addition, it will prevent disruptions to and the misuse of College electronic communications resources, services, and activities. This policy will cover acceptable use, authorized users, procedures for restricting or denying use of its electronic communication services, and the adjudication of complaints. References might be made to supplemental policies, standards, and procedures; all of those documents can be found for internal use on SMC Wired and for external viewing at www.swmich.edu.

2.0 Definition

Electronic Communications Resources: Telecommunications equipment, transmission devices, electronic video and audio equipment, encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation that supports electronic communications services.

College affiliates: any named or unnamed party interacting with the institution such as community members, vendors, service providers, subcontractors, alumni, and retirees.

Emergency Circumstances and Compelling Circumstances: Circumstances in which failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of College policies.

Authorized User: is defined as an individual who has been assigned a login ID and password by the Office of Information Technology staff, or by an authorized agent.

3.0 Roles - Responsibilities

This policy is issued by the Chief Information Officer, approved by the Information Security Committee, and to be implemented by the Information Security Program.

4.0 Applicability

This policy applies to all students, faculty, staff, as well as college affiliates. This policy applies to all SMC user accounts, private information, applications, programs, electronic communications equipment and data contained on those systems or traversing the SMC network.

5.0 Policy Area -Acceptable Use

Use of the College's electronic communication resources must occur within the parameters defined by this policy and its accompanying standards of appropriate use. These resources, which include, but are not limited to, computers, servers, networks, electronic mail and telephone services, data and data storage systems, and mobile devices, may only be used for the advancement of the College's mission. All such use

must comply with applicable federal and state laws and regulations, SMC policies, and the college's IT contracting and licensing agreements.

Standards of Acceptable Use will be established, revised, updated, and republished yearly along with the annual Information Security Review. These standards, which define appropriate and acceptable use of the College's electronic communications resources, are designed to protect these resources and the College while promoting compliance with all applicable IT-related laws, regulations, policies, contracts and licensing agreements. Authorized Users of the College's electronic communication resources must affirm their knowledge of this policy and its associated standards of appropriate use at the beginning of their professional relationship with the College and periodically thereafter, as determined necessary and appropriate by the CIO. Principles guiding the Standards of Acceptable Use to ensure appropriate, ethical and legal use of the College's electronic communication resources are as follows:

1. Maximum respect for privacy, personal rights, and public safety should be adhered to.
2. Authorization for access should only be given by the appropriate supervisor, system / data owner, or by one or more appropriate and accountable persons with the necessary steps taken to minimize any conflicts of interest.
3. Authorized access should occur only for legitimate purposes, by the authorized user with the authorized user's account only for the electronic communication resources the user is authorized to use.
4. Access should be limited to the minimum electronic information necessary to accomplish their purpose.
5. Sufficient records should be kept to enable appropriate review of compliance with this policy.

5.1 Policy Area – Authorized Users

Each authorized user is responsible for using and maintaining their access credentials in a safe and appropriate manner that protects the security of the College. Each Authorized User is charged with protecting the integrity of their personal access credentials from loss or unauthorized use. The careless or intentional misuse of access credentials is a serious violation of this policy that may result, as with other violations of Electronic Communication Policy, in disciplinary action up to and including termination of employment, or in cases of student misconduct, expulsion from SMC. Users will be categorized accordingly:

A. **College User.** College students, faculty, staff as well as college affiliates such as vendors and service providers, subcontractors, alumni, and retirees.
B. **Public user.** Persons and organizations not deemed a College User may only have access to electronic communications resources and services under programs sponsored by SMC, and as authorized by the college President, or Cabinet for purposes in accordance with section 5.1 Acceptable Use.

5.2 Policy Area

Restricting or Denying use of Electronic Communication Services Eligibility to access or use SMC electronic communications services or electronic communications resources, when provided, is a privilege accorded at the discretion of the college. This privilege is subject to the normal conditions of use, including procedures for initiation and termination of service eligibility, established by the manager of the individual electronic communications resource.

SMC reserves the right to restrict access to electronic communication resources at its discretion when required by and consistent with law, when there is substantiated reason to believe that violations of SMC policies have taken place, when there are compelling circumstances, under time-dependent critical operational circumstances, or deemed to be harassment, the proliferation of unsolicited emails, pose a cybersecurity threat, or doxing (see Definitions in section 2.0). Restriction of use is subject to established campus wide procedures or, in the absence of such procedures, to the approval of the appropriate Vice President(s) or, the SMC President, and the Chief Information Officer. Electronic communications resource providers may, nonetheless, restrict use of College electronic communications systems and services on a temporary basis as needed in Emergency Circumstances and Compelling Circumstances (see Definitions in Section 2.0).

While the College is committed to preserving the confidentiality, integrity, and availability of SMC information covered under the Secure Information Policy, when compelled to disclose an Authorized User's electronic records in response to various legal mandates, including search warrants, court orders, subpoenas, discovery requests related to litigation, and public records requests under Michigan law the College will proceed as appropriate. The College reserves the right to monitor and inspect usage records or data—including account activity, content, and devices—as necessary to fulfill its legal obligations or to effectively administer its Electronic Communication Resources. The College may disclose the results of such monitoring or inspections to appropriate authorities in furtherance of meeting its administrative or legal obligations and may use such information in disciplinary proceedings. When necessary to protect from an imminent threat to other Authorized Users or the College's infrastructure, or to prevent or respond to a violation of law or policy, the College may without notice take actions necessary to manage the threat and to preserve access to or the security of data. Such actions may include, but are not limited to, changing passwords, rescinding access rights, blocking IP's or email accounts, disabling or impounding computers, or disconnecting specific devices or segments of the College's networks, along with the implementation of other electronic/physical controls.

If it is believed there has/had been a violation of the Electronics Communication Policy a substantive due process will be followed for restricting access control:

A. Evidence Acquisition
    a. A formal request will be submitted to the SMC Chief of Staff (see Security Incident Reporting Form) .
    b. The requestor for the investigation cannot be the approver, in order to remove any conflicts of interest.
    c. Retrieval will be provided by a non-system administrator and in-the-case where no appointed personnel stands the CIO will perform such duties.
    d. Approvers will not receive the information garnered from the investigation directly, instead the information will be provided directly back to the Chief of Staff for a formal review.
B. Evidence Examination
    a. Examination of the evidence shall take place by Southwestern Michigan College Information Security Committee, whereas the committee is not available, or time does not permit, the Chief of Staff, CIO, and another Cabinet member will provide a judgement.
C. Documentation, reporting, and actions taken:
    a. The investigation shall be documented, and reported to the appropriate person/s within the College and outside the College if applicable.
    b. Suitable steps shall be taken to prevent further inappropriate use of SMC electronic communication resources as needed.
    c. Lastly the College is under no obligation to contact violators of the Electronic Communication Policy.

The CIO may temporarily suspend or permanently revoke an individual's access to the College's electronic communication resources if necessary, to protect or maintain the integrity or security of the College's network, systems, or data. However, whenever this happens a full investigation will take place subsequently within a reasonable timeframe. Authorized Users shall fully cooperate with any investigation of abuse or misuse.

5.3 Policy Area – Adjudication of Complaints

The College is committed to open discourse, the free expression of viewpoints and beliefs, and academic inquiry without unwarranted institutional intrusion. These core values must at times be balanced against or tempered by rights of others to privacy, freedom from intimidation or harassment, protection of intellectual property, and the stewardship of data, information and State of Michigan resources. Use of the College's Electronic Communication Resources is a privilege granted to Authorized Users in furtherance of their educational opportunities or professional duties and responsibilities. However, in the event an individual or organization feels that they have been wrongly accused the following process will be followed:

A. The Requestor shall submit a written request either electronically at (https://cm.maxient.com/reportingform.php?SWMichiganCollege) using the option "Information Security" in the 'Nature of this Report' field or mailed directly to the Chief of Staff

B. The request shall be presented to the Southwestern Michigan College Information Security Committee, whereas the committee is not available or time does not permit, the Chief of Staff, CIO, and another Cabinet member will provide a judgement.
C. SMC will respond within 30 days of the completion of concern.

6.0 Compliance

Students, staff, and faculty, and college affiliates are subject to this policy are also subject to the SMC Catalog, the SMC Employee Handbook, conditions of service documentation, and as well as applicable sanctions under applicable laws.

7.0 Applicable Forms

Security Incident Reporting Form (Appendix A)
Standards of Acceptable Use
Information Security Review

8.0 References

Electronic Communication Policy
(University of California, 2005)

NAU Information Security Policy.
(Northern Arizona University Policy Manual – Policy NAU-700 Rev. 2, 2013).

Customer Information Security Program Policy and GLBA Policy.
(University of Georgia).

Electronic Communications Privacy Act of 1986

Communications Assistance for Law Enforcement Act (CALEA) of 1994

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, 2005, 2006, 2011

Gramm-Leach-Bliley Act: Section 501 & 502(b)(2)

Special Publication (NIST SP) - 800-171

Appendix A

Security Incident Reporting Form

Instructions: This form is to be completed as soon as possible following the detection or reporting of an Office of Information Technology (OIT) security incident. All items completed should be based on information that is currently available. This form may be updated and modified if necessary.

1. **Contact Information for this Incident**

   Name: _____

   Title: _____

   Program Office: _____

   Work Phone: _____

   Email Address: _____

2. **Incident Description**

   Provide a brief description: _____
   _____

3. **Impact / Potential Impact** Check all of the following that apply to this incident.

   ☐ Loss / Compromise of Data

   ☐ Damage to Systems

   ☐ System Downtime

   ☐ Financial Loss

   ☐ Other Organizations' Systems Affected

   ☐ Damage to the Integrity or Delivery of Critical Goods, Services or Information

   ☐ Violation of legislation / regulation

   ☐ Unknown at this time

4. **Sensitivity of Data / Information Involved** Check all of the following that apply to this incident.

   Sensitivity of Data Definitions

Category	Example
Public	This information has been specifically approved for public release by Public Relations department or Marketing department managers. Unauthorized disclosure of this information will not cause problems for Department of Public Welfare, its customers, or its business partners. Examples are marketing brochures and material posted to Department of Public Welfare web pages. Disclosure of agency information to the public requires the existence of this label, the specific permission of the information Owner, or long-standing practice of publicly distributing this information.

Internal Use Only	This information is intended for use within Department of Public Welfare or between agencies, and in some cases within affiliated organizations, such as business partners. Unauthorized disclosure of this information to outsiders may be against laws and regulations or may cause problems for the Department of Public Welfare, its customers, or its business partners. This type of information is already widely distributed within the Department of Public Welfare, or it could be so distributed within the organization without advance permission from the information owner. Examples are an agency telephone book and most internal electronic mail messages.
Restricted/Confidential (Privacy Violation)	This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations, or may cause significant problems for the Department of Public Welfare, its customers, or its business partners. Decisions about the provision of access to this information must be cleared through the information owner. Examples are customer transaction account information and worker performance evaluation records. Other examples include citizen data and legal information protected by attorney-client privilege.
Unknown/Other	Describe in the space provided.

☐ Public

☐ Internal Use Only

☐ Restricted / Confidential

☐ Unknown / Other - please describe: _____

Provide a brief description of data that was compromised:

_____

_____

5. Who Else Has Been Notified?

Provide Person and Title: _____

6. What steps Have Been Take So Far? Check all of the following that apply to this incident.

☐ No action Taken

☐ System Disconnected from network

☐ Updated virus definitions & scanned system

☐ Restored backup from tape

☐ Log files examined (saved & secured)

☐ Other – please describe: _____

_____

Provide a brief description: _____

7. Incident Details

Date and Time the incident was discovered: _____

Has the incident been resolved? _____

Physical location of affected system(s): _____

Approximate number of sites affected by the incident: _____

Are non-Commonwealth systems, such a business partners, affected by the incident? (Y or N – if Yes, please describe): _____

Please provide any additional information that you feel is important but has not been provided elsewhere on this form: _____
_____
_____