Title/Subject: **INFORMATION SECURITY POLICY**

Applies to: ☒ faculty ☒ staff ☒ students ☒ student employees ☒ visitors ☒ contractors

Effective Date of This Revision: January 21, 2016

Contact for More Information: Office of Information Technology

☐ Board Policy ☒ Administrative Policy ☒ Procedure ☒ Guideline

---

PURPOSE

Central Michigan University ("CMU") has adopted the following Information Security Policy ("Policy") as a measure to protect the confidentiality, integrity and availability of Institutional Data as well as any Information Systems that store, process or transmit Institutional Data. This policy applies broadly to all Institutional Data, regardless of its form (electronic - in an IT system, physical - on paper, or ephemeral - a voice conversation), and applies to all faculty, staff, students and third-party Agents of the University as well as any other CMU affiliate who is authorized to access Institutional Data.

PRINCIPLES

- Supporting its mission as an educational institution, CMU puts its people first. We recognize that the faculty, staff and students within our community are our strongest security asset, but also our greatest vulnerability.
- CMU's approach to information security is nuanced. As our data becomes more sensitive and requires more protection, we augment that protection with additional administrative, technical, and physical controls.
- CMU's approach to information security allows our faculty, staff and students the rights to bring their own devices and to enjoy relatively liberal access to CMU data, but also emphasizes their responsibility to exercise good, well-informed judgment in their use of CMU's systems and data.
- CMU maintains policies, guidelines, standards and other documents (see "Additional Information" below) to bring structure to our strategy and to act as resources for our faculty, staff and students.

POLICY STATEMENTS

(to be supported by Protocols and Standards as appropriate, see "Additional Information" below)

1. Throughout its lifecycle, all Institutional Data shall be protected in a manner that is considered reasonable and appropriate, as defined in documentation approved by the Technology Planning Council ("TPC") and maintained by the Chief Information Security Officer ("CISO"), given the level of sensitivity, value and criticality that the Institutional Data has to the University.
2. Any Information System that stores, processes or transmits Institutional Data shall be secured in a manner that is considered reasonable and appropriate, as defined in documentation approved by the TPC and maintained by the CISO, given the level of sensitivity, value and criticality that the Institutional Data has to the University.

Authority: George E. Ross, President
History: none
Indexed as: cybersecurity, data management, data security

3. Individuals who are authorized to access Institutional Data shall adhere to the appropriate Roles and Responsibilities, as defined in documentation approved by the TPC and maintained by the CISO.

RESPONSIBILITY FOR COMPLIANCE

Task	Cabinet	CIO	CISO	TPC	SIRT	IT Staff	Faculty	Staff	Students
Maintenance of Policy	A	C	R	C	C	C	I	I	I
Maintenance of Standards and Guidelines		C	R	A	C	C	I	I	I
Training and Awareness		A	R	I	C	C, R	I	I	I
Design of Controls		A	R	I	C	C	C	C	C
Implementation of Controls		I	A	I	C, R	C, R	R	R	R
Monitor and Audit Controls		A	R	I	C	R			

R = Responsible - The person who actually carries out the task

A = Accountable - The person who is ultimately accountable for the task being completed appropriately

C = Consulted - People who are not directly involved in carrying out the task, but are consulted during its completion

I = Informed - Those who receive output from the task with opportunity to comment or need to be informed of its progress or completion

RISK ASSESSMENT

The Office of Information Technology will regularly, and routinely, assess risk to the university's technology environment. To accomplish this, risk assessment activities targeting specific systems, technologies, and/or operations will take place annually, while a full information security risk assessment will be conducted every third year. Results of these assessments will be used to inform OIT planning and protections and will be shared with CMU's Enterprise Risk Committee and other relevant committees.

ENFORCEMENT

Enforcement of this policy will be managed by the CISO under the guidance of the TPC. Violations of this Policy may result in suspension or loss of the violator's use privileges with respect to Institutional Data and CMU-owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with CMU. Civil, criminal and equitable remedies may apply.

EXCEPTIONS

Exceptions to this Policy must be approved by the CISO under the guidance of the TPC and formally documented. Policy exceptions will be reviewed by the TPC on a periodic basis for appropriateness.

DEFINITIONS

- **Agent**, for the purpose of this Policy, is defined as any third party that has been contracted by CMU to provide a set of services and who accesses, stores, processes, or transmits Institutional Data as part of those services.

- **Technology Planning Council** is a committee chaired by the Chief Information Officer ("CIO"). Members include the Chief Information Officer; the Chief Information Security Officer; the Deputy CIO; representatives from the Office of the General Counsel, the Enrollment and Student Services Division, the Financial and Administrative Services Division, University Communications, and Alumni and Development, all appointed by their respective office or divisional heads; the Vice President for Global Campus or designee; the Vice President for Research; and two academic officers appointed by the Provost.
- **Information System** is defined as any electronic system that stores, processes, or transmits information
- **Institutional Data** are defined as any data (digital or physical) that are owned or licensed by the University, including "University's information" as defined in the Data Stewardship Policy as:
    - "The University's information includes, but is not limited to, any physical or digital information within its purview, including information which it may not own but which is governed by laws and regulations to which the University is held accountable. It includes all student record data, all personnel data, research data (including that collected from human and animals), all University financial data, all student life data, all departmental administrative data, all alumni and donor data, all library circulation data, medical data protected under HIPAA and ADA legislation, and all other data that pertain to, or support the administration of, the University. These data may be facts, records, reports, planning assumptions, or any information meant only for internal use and /or subject to confidentiality agreements."
- **Technical Controls** are defined as digital (as opposed to physical) controls applied to information systems and technologies – for instance, the requirement to enter a password on login is a technical control.

MAINTENANCE

This Policy will be reviewed by the CISO every 5 years or as deemed appropriate based on changes in technology or legal or regulatory requirements.

ADDITIONAL INFORMATION

Questions or concerns related to this Policy should be directed to CMU's CISO at 989.774.7445. Additional information can also be found using the following resources:

- Data Stewardship Policy
- Global ID Password Policy
- Secure Configurations Policy - Workstations
- Responsible Use of Computing
- SAP Security – Authority, Rights and Responsibilities
- Web Policy
- Social Security Number Policy
- Computer Disposal Policy
- Accepting Credit Card Payments
- Identity Theft Red Flags
- HIPAA Policies – see Chapter 12
- Security-Related Protocols and Standards