

Title/Subject: **DATA STEWARDSHIP**

Applies to: faculty staff students student employees visitors contractors

Effective Date of This Revision: December 1, 2008

Contact for More Information: Office of Information Technology

Board Policy Administrative Policy Procedure Guideline

I. PURPOSE

Information is one of the University's most vital assets. The purpose of the Data Stewardship Policy is to protect this asset by setting forth the responsibilities of faculty, staff, and students for establishing and maintaining the security of the University's information; by establishing requirements for protecting personal, non-public information; and by establishing requirements for notifying individuals whose personal, non-public, information may have been disclosed by a security breach. The Data Stewardship Policy applies to all University faculty, staff, and students. This policy encompasses the safekeeping of the University's information in whatever physical form (such as printed, audio, video and electronic) it may exist, now or in the future.

II. POLICY STATEMENT

It is the policy of the University to protect its information assets and allow the use, access and disclosure of such information only in accordance with University interests and applicable laws and regulations. All University faculty, staff, and students providing services involving, or working with, the University's information are responsible for protecting it from unauthorized access, modification, destruction or disclosure.

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. This policy applies to all university data, including all archived and existing data. OIT can help to discover and protect archived and sensitive data.

III. IMPLEMENTATION

All CMU academic and business offices must develop and administer information security plans that appropriately classify and protect information under their control. Templates and guidelines for the development and implementation of such plans can be obtained from the Office of Information Technology. The protection of the University's information must be part of each office's standard operating procedure. The safeguarding of Protected Personal Information is of particular importance and is addressed in Section IV of this policy. Through the Information Security Advisory Team, Internal Audit will audit each office's information security plan every two years.

Authority: M. Rao, President
History: No Prior History
Indexed as: Electronic Security; Security of Data; Breach of Computer Security; Protected Personal Information

Title/Subject: **DATA STEWARDSHIP**

Specifically, academic and business offices must:

- establish system/data access and utilization criteria
- define the criteria for archiving the information to satisfy retention requirements
- determine the value of proprietary information to the functioning of the University and define reasonable requirements for protecting the asset
- develop a workable plan for resuming operations in the event information has been destroyed
- specify information control and protection requirements to be adhered to by employees processing and using the information
- monitor compliance and enforce this policy

However, since information security measures must cover the entire flow of information throughout the University, the implementation of the information security policy cannot be delegated to only academic and business office operations. As custodians of the University's information, all employees must adhere to established procedures to ensure that they use the University's information only as required by the normal functions of their duties and that they safeguard it properly according to its sensitivity, proprietary and/or critical nature.

IV. PROTECTED PERSONAL INFORMATION

Protected Personal Information (PPI) is personally identifiable data that must be protected through contractual and/or legal specifications, as mandated by CMU's Institutional Review Board (IRB), and/or specified in state or federal law. The types of data included in the category are, but are not limited to, individual financial records, social security numbers, academic records, disciplinary records, credit card information, proprietary data protected by law or international agreement, personal intellectual property that might be housed for academic reasons on University computing resources, and research data including data and consent from research subjects. PPI does not include published directory information or information that is lawfully made available to the general public from federal, state or local government records. Any questions concerning which university data constitute PPI should be forwarded to the CMU Office of the General Counsel.

Unless required by law, approved by the appropriate vice president, or approved by IRB, Social Security numbers, credit card numbers, or other PPI must not be collected or stored. (See related policies below.)

CMU's preference is that OIT-administered systems be used to process and store digital PPI. Digital PPI may be stored on unit-administered servers if, and only if, such systems are registered with OIT through CMU's [Internet-Facing Server Registration Requirements](#). If digital PPI must be stored elsewhere in the unit, it must be password-protected or, preferably, encrypted. The university strongly encourages the use of encryption. Encryption is an easy process, and encryption software is available through the CMU Help Desk.

PPI should only be distributed through approved university email accounts (i.e. "cmich" accounts) and only using approved university email clients, including, but not limited to, Outlook and Entourage. Email containing PPI needs to reside solely within the university email system and must not be transferred or forwarded to email systems external to CMU.

University departments must regularly re-evaluate their plans for acquisition, use, and safeguarding of PPI in conformance to this policy. Templates and guidelines for the development and implementation of such plans can be obtained from the Office of Information Technology.

CMU users must report any possible exposure of PPI. Possible exposure includes any incident in which the security of a computer or physical system is compromised, including theft or loss of a computer, storage device, or any other medium on which unauthorized person(s) might be able to access, copy, or read data files containing PPI. It does not include normal use by authorized employees or University business partners.

Reports of possible exposure of PPI may be made by email to the CMU Security Incident Response Team (CMU-SIRT) at security@cmich.edu or by phone to the Chief Information Officer (CIO) in the Office of Information Technology at 989.774.1474. The CMU-SIRT and CIO will follow the procedures described in the Digital Incident Notifications Protocol,

Title/Subject: **DATA STEWARDSHIP**

[System Compromise, Loss, or Theft - Resolution Process](#), to investigate and escalate the matter appropriately. If necessary, CMU will use this same protocol to notify any affected individuals or other entities.

V. RELATED POLICIES

[Social Security Privacy Policy](#)

[HIPAA Privacy Practice Policy](#)

[HIPAA Workforce Security and Information Access Management Policy](#)

[HIPAA Workstation and Personal Security Policy](#)

[HIPAA Protected Health Information Network Policy](#)

[HIPAA: Investigation of Complaints and Reports of Breach of Privacy and Security of PHI, Sanctions for Breach of Privacy and Security PHI](#)

[HIPAA Minimum Necessary Use and Disclosure of Protected Health Information](#)

[PCI Compliance Policy](#)

[Policies of the Office of Research and Sponsored Programs](#)

- Research Integrity Policy
- IRB - Human Subjects
- IACUC- Animal Subjects
- IRC- Recombinant DND

VI. COMPLIANCE

Employees who violate this Policy may be subject to disciplinary action up to and including termination from employment.

VII. AMENDMENTS AND ADDITIONS

The CIO may approve exceptions to this policy. All amendments and additions to this policy will be drafted by a committee convened by the CIO and will be reviewed and approved by the Provost and the President. Changes in this policy will be appropriately publicized.

Central Michigan University reserves the right to make exceptions to, modify or eliminate this policy and or its content. This document supersedes all previous policies, procedures or guidelines relative to this subject.