Title/Subject: **DATA STEWARDSHIP**

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

Effective Date of This Revision: January 1, 2018

Contact for More Information: Office of Information Technology

☐ Board Policy ☒ Administrative Policy ☐ Procedure ☐ Guideline

---

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 providing common terminology for classifying that 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.

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.

ROLES AND RESPONSIBILITIES

All Institutional Data must be protected in all phases of its use and existence. This section of this policy defines the roles of Owner, Custodian (including IT professionals), Steward, and User with regard to Institutional Data. Roles and Responsibilities can be circumstantial and overlapping, and this standard is meant to help address the ways in which the roles and responsibilities differ and/or relate, and establish a common vocabulary for referring to them in Information Security terms.
Individual responsibilities and roles may differ by system used and data being accessed, and individuals may qualify as or serve in one or many roles simultaneously, depending upon their position or job, and the systems and data being used. For instance, the Vice President for Finance may be a Data Owner of the payroll system but also a Data User in the Human

---

Authority: M. Rao, President; George E. Ross, President
History: 2008-12-01;
Indexed as: Electronic Security; Security of Data; Breach of Computer Security; Protected Personal Information

Resources benefits system; a Faculty member may be a Data Owner in a scientific research project, a Data Steward of unpublished papers being peer-reviewed for others, and a Data User in the email system; and an Information Technology professional may be a Data Custodian for a database they manage on behalf of a Data Owner, and a Data User of the time & attendance system. As they enter or make changes to data in their systems, Data Owners may be acting as Users, too.

Data Owner: Usually university officers or heads of schools, divisions, departments, offices, programs, etc. Data Owners are accountable for managing, protecting, and ensuring the integrity and usefulness of Institutional Data. In addition to upholding university policies and state/federal law, Data Owners are responsible for identifying the sensitivity and criticality of data, as well as any retention requirements. Data Owners are also responsible for determining appropriate access to Institutional Data.
Data Custodian (including IT professionals): Data Custodians have control over a data asset's disposition whether stored, in transit, or during creation, and are responsible for recommending, designing, implementing, and maintaining security controls appropriate to the systems and areas they support. They are usually associated with the Office of Information Technology (OIT) units within the university and typically have modification or distribution privileges. Because they take such a hands-on role and often have elevated access privileges, Custodians carry a significant responsibility in protecting data.
Data Steward: Although they often have custodial responsibilities, Data Stewards are distinguished by having delegated decision-making authority. They may represent Data Owners in policy discussions, architectural discussions, or in decision-making forums, and have responsibility for maintaining protections and appropriate access. Stewards may also be responsible for Data created or used by multiple Users, not just themselves.
Data User: Data Users create and control Institutional Data, and share responsibility in helping Data Stewards and Custodians manage and protect data. Data Users can consist of any individuals or university units that create, use, or manage sets or parts of Institutional Data. Anyone using any University information system or accessing Institutional Data is a Data User.

Data Owners are ultimately responsible for the data in the systems (for instance, the VP of Finance is responsible for all Finance data). Custodians are responsible for the design and controls of the systems with data in them (for instance, the Server Administrator, Network Engineer, Database Administrator, Payroll Programmer, and the Finance Support Analyst may all be Custodians of the Payroll system). Stewards are Owner-delegated agents (for instance, Directors and Managers in the Finance Division under the VP of Finance, responsible for the operations, access, and use of the different Finance systems). Users access and use the systems to input and manipulate (work with) the data.

DATA CLASSIFICATION

All Institutional Data requires protection to preserve its proper confidentiality, integrity (including accuracy), and availability. This section of the policy defines three classifications of Institutional Data (Public, Protected, and Restricted) to help guide in the proper discussion and application of protective information security controls in University-owned systems and systems that process or use Institutional Data.
Generally speaking, the more controlled or sensitive the classification of data, the more protections the data requires. All systems require basic controls and some data require additional integrity, availability, and access controls, but restricted data is particularly sensitive and may be internally or externally regulated, requiring implementation of controls specific to the type of regulation in order to reduce risk to the University and mitigate for possible harmful effects from loss or exposure of the information.
While the accuracy and integrity of all data is important, Public data requires no login to access, Protected data requires a login, and Restricted data requires a login plus more. Using these terms will help ensure consistency in description and expectations when securing data.

Data Classifications (ordered least-to-most controlled, based upon risk):

Public: Least-controlled data; available to the public; no login required
Public data includes data intended to be published or shared and accessible readily or by request, to the public without login. Its availability and integrity are important to maintain, but confidentiality

concerns are low. Public data is general information about the University including but not limited to visitor information, program descriptions, campus maps, general departmental information, sports schedules, information about applying for admission and financial aid, library resources, operating hours, student directory information, course lists, class descriptions, news and events, etc. Care should be taken to ensure Protected and Restricted data is not mixed in with, or is properly redacted from Public data before it is made available to the public.

Protected: Moderately-controlled data; access restricted; login required
Protected data also requires confidentiality controls, and it may only be accessed by eligible university employees, other members of the university, and other designated individuals. Some Protected data may be further restricted to certain groups, areas, or individuals of the university. Much of the course content, performances, intellectual property, employee information, all non-directory student information, and business-specific information of the university is Protected, though some may also be released or made available to the public by the appropriate data owners, or as required of public universities. Care should be taken to ensure Restricted data is not mixed in with Protected.

Restricted: Most-controlled data; access and authorization restricted, actively monitored; login required, plus additional controls required
Restricted data also requires strong access controls and monitoring, and it may include legal, ethical or other constraints (regulation) in its access, use, processing, storage, backup/archive, and disposition/disposal. Inappropriate handling and insufficient safeguarding of Restricted data could result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, and/or other possible harmful effects. Some Restricted data is highly restricted (for instance, social security numbers when combined with full names, HIPAA-governed health information when combined with individual identifiers, or credit/payment card information, etc.) and specific control requirements and additional protective measures may vary, depending upon applicable regulatory constraints. Loss or release of highly restricted data may require additional steps to mitigate for any harmful effects (including breach alert and response measures, reporting to regulatory authorities and affected individuals, etc.).
For these reasons, Restricted data must not be stored on personally-owned devices (personal laptops or desktops) or in online services (like Google Drive or Amazon Web Services) not specifically contracted and intended by CMU for the storage of restricted data. For information about appropriate storage locations for restricted data, please contact the CMU Help Desk at 989.774.3662.
For information regarding the governance and safeguarding of workstations and systems/servers housing CMU data, see "Secure Computer Configurations Policy – Workstations" and "Secure Computer Configurations Policy – Servers."

Other Data Classifications: The University does not use the classification terms 'confidential, secret, top secret' unless they accurately describe data or information so categorized by the U.S. Government in the OMB Circular A-130 as pertaining to national security information. In general, none of the information at that level will appear in the University academic, administrative, research, and IT environment and controls required to protect such information at those levels do not apply.

A Special Note Concerning Protected Personal Information

Protected Personal Information (PPI) is Restricted, personally identifiable data that is required to 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.)
PPI should only be distributed through approved university email accounts (i.e. "cmich" accounts). Email containing PPI needs to reside solely within the university email system and, without being specifically encrypted, 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. Data Owners and Stewards are responsible for ensuring that data classifications are appropriately applied and requirements followed.
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 CMU Help Desk at 989.774.3662. The CMU-SIRT and CISO will follow established incident response procedures to investigate and escalate the matter appropriately. If necessary, CMU will use this same protocol to notify any affected individuals or other entities.

IMPLEMENTATION

Working with appropriate Data Custodians and Data Stewards, all CMU Data Owners must develop and administer information security plans that appropriately classify (see Data Classifications above) and protect the information under their control. The protection of the University's data must be part of each office's standard operating procedure. The safeguarding of Protected Personal Information is of particular importance and is addressed immediately above. Templates and guidelines for the development and implementation of information security plans can be obtained from the Office of Information Technology (OIT).

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 classification.

RELATED POLICIES AND OTHER RESOURCES:

Responsible Use of Computing Policy
Data Stewardship Policy
Information Security Policy
Computer Disposal Policy
Record Management Policy
Information Security FAQ

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.