Michigan State University
INSTITUTIONAL DATA POLICY

I. PURPOSE.

Michigan State University needs to protect the security and integrity of its Institutional Data without hindering the effective and efficient use of those Data. To achieve this objective, the best efforts of every member of the University community are required. The purpose of this Policy is to establish minimum requirements for the appropriate stewardship of Institutional Data.

II. APPLICABILITY.

This Policy applies to all members of the University community – faculty, staff, and students.

III. DEFINITIONS.

A. **Institutional Data:** Institutional Data are all of the data and records held at the University, in any form or medium, for the administration, operation, or governance of the University or any unit of the University.

B. **Confidential Data:** Confidential Data means (i) Institutional Data that could, by itself or in combination with other such Data, be used for identity theft or related crimes, (ii) Institutional Data whose public disclosure is restricted by law, contract, University policy, professional code, or practice within the applicable unit, discipline, or profession, (iii) records of the University's security measures, and (iv) Institutional Data whose value would be lost or reduced by unauthorized disclosure or by disclosure in advance of the time prescribed for its authorized public release, or whose unauthorized disclosure would otherwise adversely affect the University financially.[1]

C. **Public Data**: Public Data are Institutional Data that have become generally available to members of the public because a person with authority to do so has intentionally released or distributed them without restriction or limitation.

D. **University purposes:** University purposes are (i) the fulfillment of employment responsibilities at the University, and (ii) participation in University governance processes.[2]

---

[1] Appendix I gives examples of Confidential Data.

[2] Participation in University governance processes includes participation on University boards, bodies, governing groups, and committees through which members of the University community contribute to the operation of the University.

IV. RESPONSIBLE USE REQUIREMENTS.

Members of the University community must comply with the following requirements for responsible use of Institutional Data, provided that Sections IV(A), IV(C)(2), and IV(C)(4) do not apply to Public Data.

A. Members of the University community may access and use Institutional Data only for University purposes.

1. Members of the University community may not use or disclose Institutional Data to obtain or provide others with a private benefit that is inconsistent with the University's interests.

2. Members of the University community may alter, store, and distribute Institutional Data only for University purposes.

3. Each member of the University community may access Institutional Data only if, and then only to the extent that, he or she needs to do so for a University purpose.

B. Institutional Data must be used, stored, transferred, disseminated, and disposed of in ways that minimize the potential for their improper disclosure or misuse.

1. Members of the University community must comply with all laws, University policies, and contracts that govern the use and release of Institutional Data, especially Confidential Data.

2. Records that contain Confidential Data and are no longer needed for University purposes must be disposed of promptly and properly.[3] Best practices for record disposal are described in Appendix II.

3. Records that contain Confidential Data shall be properly secured to minimize the risk that the Confidential Data will be accessed,

[3] Michigan's Identity Theft Protection Act requires that any records that contain any of the following types of Confidential Data in an unencrypted form be destroyed (shredded or erased) when such Confidential Data is removed from a University data system and the University is not retaining the Confidential Data elsewhere for another purpose: a person's first name (or first initial) and last name in combination with that person's (a) social security number, (b) driver's license or state personal identification number, or (c) credit or debit card or other financial account number, in combination with any security code, access code, or password that would permit access to that financial account. The Identity Theft Protection Act does not require the destruction of any records needed by the University for purposes of an investigation, audit, or internal review. ~~.~~

either intentionally or inadvertently, by individuals who do not need to see or use the Confidential Data for University purposes.

C. Members of the University community are individually responsible for the security and integrity of Institutional Data in their possession or control, including their proper storage and disposal.

1. Members of the University community shall not knowingly create inaccurate or misleading Institutional Data, or deliberately alter or delete accurate Institutional Data to make those Institutional Data, or other Institutional Data, inaccurate or misleading.

2. Members of the University community may share Institutional Data only with individuals who need to access those Data for a University purpose.

3. Members of the University community are individually responsible for their own use, storage, dissemination, and disposal of the Institutional Data to which they have access.

4. Members of the University community who, for University purposes, make Institutional Data available to individuals who are not subject to this Policy should take appropriate action to provide for the proper use, storage, and disposal of those Institutional Data by those individuals, including, when necessary, contractual limitations on the further dissemination of the Institutional Data by those individuals.

V. LEGALLY MANDATED OR AUTHORIZED RELEASE.

A. This Policy does not affect MSU's obligations to release data or records when so required by law.

B. This Policy does not restrict the authority of appropriate University officials to determine the time and circumstances for the public release of Institutional Data, including Confidential Data.

C. This Policy shall not be construed to reduce the control faculty and students exercise over their own scholarly work pursuant to other University policies.[4]

D. This Policy is not intended to discourage the reporting, in good faith, of known or suspected fiscal or other misconduct or violations of law,

[4] See, e.g., the faculty's right to publish or present research findings and creative works pursuant to the Faculty Rights and Responsibilities Policy.

regulation, or University policy to the relevant University offices or to appropriate external authorities, including, without being limited to, the filing of complaints or grievances under applicable University policies, procedures, or collective bargaining agreements.

VI. IMPLEMENTATION.

Unit supervisors/unit administrators are responsible for implementing training and oversight procedures consistent with this Policy for their own units.

VII. VIOLATIONS.

Violations of this Policy may result in disciplinary action, up to and including dismissal for employees and suspension for students. Individuals who violate this Policy may also have their access to the MSU network or to certain data sources or software applications revoked. In some cases, they may also be subject to civil and criminal penalties under state or federal laws governing certain Confidential Data.

VIII. ADDITIONAL RESOURCES.

Situations may arise for which additional advice may be required. Unit-level data security administrators; Academic Human Resources; Human Resources; Vice Provost for Libraries, Computing and Technology; the Office of the Registrar; Academic Services; Enterprise Information Stewardship; University Archives and Historical Collections; the Office of Regulatory Affairs; or the Office of the General Counsel may be consulted as appropriate.

APPENDIX I

Confidential Data

Confidential Data means

(i) data that could, by itself or in combination with other such data, be used for identity theft, fraud, or other such crimes.

Examples:

- Social security numbers[1]
- Payment (credit/debit) card account numbers
- Bank account numbers, automated clearinghouse and electronic funds transfer account numbers, brokerage account numbers, and other financial account numbers
- Driver's license numbers and state resident/personal identification numbers
- Passport, visa, and alien registration numbers
- Taxpayer and employer identification numbers
- Employee and student identification numbers
- Health insurance identification numbers
- Digital keys and passcodes
- Passwords, security codes, access codes, biometric codes, personal identification numbers, and other unique account identifiers
- Personal data such as date of birth and mother's maiden name
- Digital signatures

(ii) data and records whose public disclosure is restricted by law, contract, University policy, professional code, or practice within the applicable unit, discipline, or profession.

Examples:

- Student education records[2]
- Individually identifiable data in a person's medical record
- Human subjects research data, if the subjects have been promised confidentiality
- Trade secrets or other proprietary business data owned by a third party and provided to the University upon a promise of confidentiality in a nondisclosure agreement or other contract
- Proprietary computer applications or source code to which the University holds a license that restricts further or public distribution

---

[1] See also Social Security Number Privacy Policy (www.hr.msu.edu/HRsite/Documents/Uwide/Policies/ssnPrivacy.htm).

[2] See MSU Access to Student Information Guidelines (www.reg.msu.edu).

- Exam questions and answers/scoring keys which the professor has not released as Public Data
- Bids and proposals until they are opened or the deadline for their review has passed
- Employment data such as retirement account allocations and investments and designations of beneficiaries and personal contacts
- Documentation of grievance, arbitration, and disciplinary proceedings
- Information about pending research misconduct proceedings
- Financial aid applications and related tax and financial data
- Information and records protected by the attorney-client or attorney work product privilege
- Private financial and other data disclosed under the University's conflict of interest policies
- Private financial, contact, giving, and other data about donors and prospective donors collected and maintained in connection with the University's development/advancement activities
- Criminal background check results and other data contained in a consumer report under the Fair Credit Reporting Act
- Data derived from servicing or collecting loans from the University

(iii) information about, and records of, the University's security measures.

Examples:

- Passwords for access to University facilities or computer systems
- Decryption keys
- Security codes and combinations for locks
- Key codes
- Security plans
- Security procedures
- Threat assessments and preparedness strategies
- Law enforcement deployment plans
- Operational instructions for law enforcement officers and other emergency personnel

(iv) information whose value to the University would be lost or reduced by disclosure in advance of the time prescribed for its authorized public release, or whose disclosure would otherwise adversely affect the University financially.

Examples:

- Research data or results prior to publication or the filing of a patent application
- Non-patentable technical information or know-how that enhances the value of a patented invention or that has independent commercial value
- Information relating to the University's intention to buy, sell, or lease property whose disclosure could increase the cost of that property for the

University or decrease what the University realizes from that property (e.g., real property appraisals)

- Computer applications to which the University owns the code

APPENDIX II

Best Practices for Record Disposal

Best practices for record disposal are constantly changing as the technologies that contain records evolve. Two current online resources for best practices are:

- How to Sanitize Data for Disposal and Day-to-Day Security
  http://techbase.msu.edu/article.asp?id=6567&service=help

- Best Practices in Disposal of Computers and Electronic Storage Media
  http://computing.msu.edu/msd/documents/safecomputerdisposal.pdf

Paper records should be shredded using a cross-cut shredder, or packaged for confidential shredding by a University or commercial service in a locked confidential records container made available for this purpose.