University Advancement Data Policy

I. PURPOSE

Michigan State University seeks to protect the security and confidentiality of its Institutional Data without hindering the effective and efficient use of that 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 responsible use requirements for University Advancement Data. This Advancement-specific policy statement is consistent with and follows from the MSU Data Policy.

The following policy applies to requesting and receiving information from the University Advancement System at Michigan State University. This Policy does not prohibit the use of confidential data where the use is authorized or required by state or federal statute, rule, regulation, or court order or rule, or pursuant to legal discovery or process.

II. APPLICABILITY

This Policy applies to all members of the University community – faculty, staff, students, and volunteers. Official uses of data from the system include acquiring and distributing alumni, donor or prospective donor information (through database access and data sets) for the support of approved University-related activities. As a Michigan State University employee, or an agent of the University acting on behalf of the University, you agree to abide by this policy.

III. DEFINITIONS

A. University Advancement Data

Information and records that members of the MSU community collect, create, store, distribute, and use in the normal course of business. This Policy applies to all Advancement Data on behalf of MSU maintained in any form or media, including paper and electronic (i.e. phones, PDA's, laptops, thumb drives, and other electronic storage devices.)

B. Confidential Information

1. Information or records that could be used for identity theft or related crimes (i.e. more than the last 4 digits of credit card and/or checking account numbers; driver's license numbers; and social security numbers; name in conjunction with birth date)

2. Information or records whose public disclosure is restricted by law, contract, University policy, professional code, or practice within the applicable discipline or profession.[1] i.e. donor (e.g. biographical information including address, phone, email, title, related organizations, etc)., donation (e.g. amount, form of gift,

designation, etc.) and prospect (e.g. estimated gift capacity, self-reported wealth or asset information, file notes, etc.) information.

C. Proprietary Information

Proprietary information means information, records, or data whose value would be lost or reduced by disclosure, or by disclosure in advance of the time prescribed for its authorized public release, or whose disclosure would otherwise adversely affect the University financially.

IV. RESPONSIBLE USE REQUIREMENTS

Members of the University community must comply with the following responsible use requirements for Advancement Data.

A. University Advancement Data may only be used for University business.

1. Members of the University community may only access confidential or proprietary information necessary to perform or complete their own work assignments and responsibilities.

2. Members of the University community shall exercise care regarding Advancement Data acquired, used or available for use in the course of their employment with the University. Members of the University community shall not use or disclose such information for personal gain or benefit.

3. Members of the University community shall access, create or alter Advancement Data only as authorized and permitted within their job responsibilities.

4. Members of the University community shall not knowingly create inaccurate or misleading Advancement Data, or deliberately alter or delete accurate Advancement Data to misrepresent facts.

5. University employees should not give any address, telephone, email, or other information from the database to non-University persons unless deemed appropriate by University administrators, even if portions of such information may otherwise be considered public.

6. As a matter of policy and for privacy considerations, University Advancement does not provide alumni contact information to the general public or alumni. Requests of this type should be directed to the Alumni Association or to the following website which identifies "Resources for Finding Alumni". http://www.msualum.com/find/Locator.cfm

7. All requests for information from members of the media must be forwarded immediately to University Relations.

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

1. Members of the University community must comply with all laws, University policies, and contracts that govern the use of confidential and proprietary information.

2. Records that contain confidential or proprietary information and are no longer needed to conduct University business or to meet document retention policies must be disposed of promptly and properly. Paper documents must be shredded. Electronic documents should be destroyed in a manner consistent with the "best practices" guidance issued by the Vice Provost for Computing and Technology.
http://lct.msu.edu/documents/computerdisposal.pdf

3. Records that contain confidential or proprietary information shall be properly secured so that those records are accessed only by individuals with a legitimate University business reason. University Advancement, through the Director of Advancement Systems, restricts access to information or documents containing *confidential* data to those employees who have a legitimate University related business purpose to access such information or documents. Unit supervisors/unit administrators are responsible for implementing this restriction through appropriate unit training, security rights and oversight procedures.

C. When dealing with confidential information identified in III.B.1 above (i.e. identifying numbers).

1. Confidential data in printed documents must be redacted unless there is a business reason not to (i.e., original personnel forms). Drawers containing confidential data that is NOT redacted must be locked each night – even if located in a locked office. (**Redacted** – confidential data blacked out so that data is unreadable.)

2. Except in management approved cases, confidential data must NEVER be printed on a report.

3. Gift/pledge documentation used in gift or pledge processing will be scanned and then destroyed. The scanned image is protected and viewable by authorized personnel only by virtue of the security within the imaging system. When scanned, the sensitive/confidential data is redacted.

4. Any confidential data that must be stored will be encrypted. The data should be purged after it has served its purpose. No confidential data should be stored on the LAN, a removable drive or a PC's hard drive, or portable devices. PDA's, laptops, smart phones, etc. should NEVER hold sensitive/confidential data.

5. Do not send (or ask others to send) confidential data via email. Credit card numbers can be faxed to University Advancement as long as the receiving fax machine (517-432-1129) is located in a secure area. Once the confidential data is used for business purposes it must be redacted and/or destroyed.

6. Do not keep multiple copies of documents with sensitive/confidential data unless there is a business reason. Determine where it makes most sense for a copy to reside and keep it only in that place. For example, purchasing card applications are kept centrally in Budgets and Gift and Data Services, so they should not be retained elsewhere.

D. When dealing with confidential information identified in III.B.2 above

1. Any data should be purged after it has served its purpose. Once the data is used for business purposes it must be shredded. Confidential data should not be downloaded to portable devices, (i.e. PDA's, laptops, smart phones, thumb drives, etc.)

2. Do not keep multiple copies of documents with data unless there is a business reason. Determine where it makes most sense for a copy to reside and keep it only in that place.

E. Members of the University community are individually responsible for using and releasing Advancement Data appropriately.

1. Members of the University community may not provide confidential or proprietary information to individuals who do not have a legitimate University business reason to access such information.

2. Members of the University community are individually responsible for maintaining the security and integrity of Institutional Data under their control. Electronic access is granted using a unique login and password. It is the responsibility of the user to protect his/her password at all times. It is NOT to be shared or allowed to be used by another person. The password will be changed on a periodic basis.

3. University personnel with approved access to constituent data may contract the services of outside vendors (e.g., data processing consultants, direct mail firms, etc. to process and/or distribute

information obtained from the constituent database for the above purposes. Prior to entering into a vendor agreement, contact the Director of Advancement Systems for review to ensure that the contract complies with the policy. The preferred method of vendor data access is through a VPN or secure FTP services with the data stored in a central location. If this is not possible, the data may be emailed if encrypted or zipped with a password. The following policies apply to all outside vendor data use and/or distribution:

a. The vendor must agree to use the information only for the purpose specifically intended by the university client.

b. The sale or transfer of the information by the vendor is strictly prohibited.

c. In all cases involving the use of outside vendors or contractors, the absolute confidentiality of the information provided from the MSU constituent database is the responsibility of the university client.

d. Misuse will be referred to legal counsel for possible further action.

V. PROHIBITED DISCLOSURES

Employees of or working on behalf of University Advancement shall maintain the confidentiality of institutional data and documents containing *confidential data.* Employees shall not do any of the following with *confidential data:*

A. Publicly display the *confidential data.

B. Visibly print the *confidential data* on any identification badge, membership card, permit or license.

_____

*"Publicly display" means to exhibit, hold up, post or make visible or set out for open view, including but not limited to, open view on a computer device, computer network, website or other electronic medium or device, to members of the public or in a public manner.
"Mail" includes delivery by United States mail, campus mail or any other delivery service that does not require the signature of the recipient indicating actual receipt.

C. Require an individual to transmit his/her *confidential data* over the Internet or a computer system or network unless the connection is secure, or the transmission is encrypted.

VI. 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 be subject to the civil and criminal penalties provided for in state or federal laws governing confidential or proprietary information.

VII. ADDITIONAL RESOURCES

Situations may arise for which additional advice may be required. Questions regarding this policy may be directed to the Directors of Advancement Systems or Human Resources and Training at University Advancement.

Appendix I.
CONFIDENTIAL AND PROPRIETARY INFORMATION

1. Confidential Information
   Examples of confidential information include but are not limited to:
   - Social Security numbers (SSNs) – the use of which is controlled by the Michigan Social Security Number Privacy Act, and institutional policy (www.ssnpolicy.msu.edu)
   - Payment (credit/debit) card account numbers and related information
   - Bank account numbers, Automated Clearinghouse (ACH), Electronic Funds Transfer (EFT) account numbers and related information
   - Driver's license numbers
   - Names, addresses and phone numbers when used in conjunction with any of the above data and other personal data such as date of birth, mother's maiden name, or when restricted or protected by the individual
   - Information or records whose public disclosure is restricted by law, contract, University policy, professional code, or practice within the applicable discipline or profession. (i.e. donor, donation and prospect information)
   - Student educational records – as defined and governed by the Family Educational Rights and Privacy Act (FERPA) and MSU's Guidelines Governing Privacy and Release of Student Records (www.reg.msu.edu), including student number and student name pairings
   - Proprietary information owned, used, or in the possession of the University, such as computer applications for which MSU owns the code or a license, or other intellectual property
   - Employment data such as benefits enrollment, beneficiary data, and certain grievance, arbitration, or legal proceedings documentation

2. **Proprietary Information**
   Examples of proprietary information include but are not limited to:
   - Information about the University's intention to buy, sell, or lease property whose disclosure would increase the cost of that property for the University or decrease what the University realizes from that property.