

**MICHIGAN STATE**  
**U N I V E R S I T Y**

**GUIDELINES FOR INTERNAL AND EXTERNAL REPORTING OF DATA SYSTEM SECURITY BREACHES**

**I. PROCEDURES FOR INTERNALLY REPORTING A SUSPECTED COMPROMISE OF A DATA SYSTEM**

**What is a Reportable Incident**

A reportable incident occurs when (a) an unauthorized person is believed to have gained the ability to access confidential or proprietary data that are stored on a University data system, or (b) a person who is authorized to access confidential or proprietary data that are stored on a University data system misuses that data.

**Confidential and Proprietary Data**

Confidential data and proprietary data are terms that are defined in the University's Institutional Data Policy (in draft). Confidential and proprietary data include:



**Libraries, Computing and Technology**

OFFICE OF THE  
PROVOST

David A. Gift  
*Vice Provost*

Michigan State  
University 400 Computer  
Center.  
East Lansing, MI  
48824-1042

Voice: 517-353-0722  
FAX: 517-432-1430  
gift@msu.edu

1. Social security number;
2. Credit card number or debit card number;
3. Bank account number, automated clearing house number, or electronic funds transfer account number;
4. Driver's license number;
5. Name, address, and date of birth, when all three are used together;
6. Mother's maiden name;
7. Student records that are protected by the Family Educational Rights and Privacy Act (FERPA) or the University's Guidelines Governing Privacy and Release of Student Records;
8. Protected health information under the Health Insurance Portability and Accountability Act (HIPAA);
9. Research data or results prior to publication or the filing of a patent application;
10. Information subject to a contractual confidentiality provision; or
11. Security codes, combinations, and passwords.

## **How to Report**

### Department/Unit Responsibilities

The department or unit responsible for the affected data system will immediately inform the Academic Technology Services' (ATS) network security team of the reportable incident (this contact should be made through the ATS Helpdesk, 432-6200; follow the recorded instructions for reporting a "security incident"). ATS will alert the Department of Police and Public Safety (DPPS). DPPS will determine whether a criminal investigation is warranted. When there is no criminal investigation, or upon completion of a criminal investigation, ATS will resume coordination of the incident.

The department or unit will facilitate investigation of the reportable incident by:

- Immediately disconnecting the affected systems from the network, but leaving them powered on, until investigators direct otherwise;
- Not logging on or performing administrative functions on the affected system until investigators arrive; and
- Recording all actions taken in connection with the discovery of the reportable incident – in writing, indicating date and time.

### Reporting Responsibilities

ATS will immediately report the incident to the Vice Provost for Libraries, Computing and Technology (LCT). The Vice Provost will notify the President, Vice President for Finance and Operations, Provost, General Counsel, Vice President for University Relations, Secretary to the Board of Trustees, and Director of Internal Audit of any significant reportable incident.

ATS also will promptly report the incident to the following offices depending on the type of confidential or proprietary data that is involved:

- Credit or debit card data – Controller's Office
- Student records – Registrar's Office (Associate Provost for Academic Services)
- Research, intellectual property, or export-controlled data – Regulatory Affairs, Vice President for Research and Graduate Studies
- Protected health information – HIPAA Officer
- Employee records – Human Resources.

These offices are responsible for notifying external parties (e.g., payment card companies and governmental agencies) if appropriate.

## **II. PROCEDURES FOR EXTERNAL NOTICE OF A SECURITY BREACH**

Michigan's Identity Theft Protection Act, MCLA 445.63, prescribes when the University must give to Michigan residents notice of a security breach of a University data system that contains their personal information.

### **What Is A Security Breach**

A security breach means the unauthorized access and acquisition of data from a University data system that compromises the security or confidentiality of a person's personal information.

Access is not unauthorized if:

1. The employee or other person acted in good faith in accessing the data;
2. The access was related to the activities of the agency or person; and
3. The employee or other person did not misuse any personal information or disclose any personal information to an unauthorized person.

### **What Is Personal Information**

Personal information means a person's first name or first initial and last name in combination with any of the following data elements when the data elements are not encrypted:

1. Social security number;
2. Driver's license number; or
3. Account number, credit or debit card number, or other financial account number, in combination with any required security code, access code, or password that would permit access to a person's financial account.

Personal information does not include government records or documents lawfully made available to the general public.

### **Is Notice Required**

The University must give notice when it discovers a security breach if:

1. The resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person; or
2. The resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.

The above notice is not required if the security breach has not caused, or is not likely to cause, substantial loss or injury to, or result in identity theft with respect to, one or more Michigan residents.

### Determining Whether Notice Is Required

In determining notice is required, University administrators will consider the following questions:

1. Is the medium or device storing personal information in the physical possession or control of an unauthorized person (e.g., a lost or stolen computer)?
2. Is there credible evidence that personal information has been downloaded or copied?
3. Was personal information used by an unauthorized person (e.g., opening fraudulent accounts or identity theft)?
4. Was the intrusion stopped while in progress, or before personal information could be acquired?
5. Is there credible evidence that the purpose of the intrusion was to seek and collect personal information?
6. Is there credible evidence that the medium or targeted device was used, or being prepared for use, for malicious purposes other than accessing and acquiring personal information (e.g., storage and distribution of large data files)?
7. What is the likelihood that the intruder has obtained data in a usable format?

When the University discovers a data system security breach that may require notice, the following University administrators will decide whether to notify potentially affected persons: President, Vice President for Finance and Operations, Provost, General Counsel, Vice President for University Relations, Vice Provost for LCT, and Chief of Police.

### **When And How Must Notice Be Given**

In the event that University administrators determine that the University must notify potentially affected persons of a data system security breach, the following procedures will be used.

The University will notify potentially affected persons, without unreasonable delay after detection of the security breach, in writing, by U.S. mail, or electronically (by e-mail) if the University has an e-mail address for the potentially affected person.

The University also will conspicuously post a notice on the University website and notify major statewide media in the form of a press release if:

1. The cost of giving the notice described above exceeds \$250,000;
2. More than 500,000 Michigan residents must be notified; or

3. The University has insufficient contact information to notify potentially affected persons.

The University will attempt to notify all potentially affected persons, regardless of their Michigan residency status.

The University may delay notification if:

1. A delay is necessary for the University to assess the scope of the security breach and restore the reasonable integrity of the data system; or
2. DPPS or another law enforcement agency determines and advises that notification will impede a criminal or civil investigation or jeopardize homeland or national security.

However, the University must give the required notice without unreasonable delay when the reason for the delay no longer exists.

### **Content of Notice**

The department(s) or unit(s) responsible for the data system affected by the security breach will prepare the notice, with the assistance of LCT, for review by appropriate University administrators.

The notice must clearly and conspicuously:

1. Describe the security breach in general terms;
2. Describe the type of personal information that is the subject of unauthorized access or use;
3. If applicable, generally describe what the University has done to protect the data from further security breaches;
4. Include a telephone number where a notice recipient may obtain assistance or additional information; and
5. Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft.

### **Providing a Toll-Free Number**

If a press release is issued, University Relations will provide a toll-free number for potentially affected persons to call to obtain additional information. The unit or department responsible for the data affected by the security breach will field the calls and provide information from a FAQ sheet. If a large number of calls is anticipated, the University may contract with an external agency to respond to calls.

The department(s) or unit(s) responsible for security of the data system will bear all costs associated with notification and any fines that may be levied under Michigan's Identity Theft Protection Act, MCLA 445.63.

### **Destruction Of Data**

The University will destroy any data that contain personal information concerning a person when that data are removed from a data system and the University is not retaining the data elsewhere for another purpose not prohibited by state or federal law. These guidelines do not prohibit the University from retaining data that contain personal information for purposes of an investigation, audit, or internal review.

Original Guidelines published 28 January 2006

Guidelines revised for compliance with MCLA 445.63, 14 June 2007

Guidelines revised to correct for Academic Technology Services unit name, 24 February 2009

Guidelines revised regarding network attachments, 16 July 2009