

MICHIGAN STATE UNIVERSITY

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 is stored on a University data system, or (b) a person who is authorized to access confidential or proprietary data that is 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 Confidentiality Policy for Institutional Data. Confidential and proprietary data include:

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;
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 Computing and Network Services' (ACNS) network security team of the reportable incident (this contact should be made through the ACNS

**LIBRARIES
COMPUTING &
TECHNOLOGY**
Michigan State University
400 Computer Center
East Lansing, MI
48824-1042
517/353-0722
FAX: 517/432-1430

Helpdesk, 432-6200; follow the recorded instructions for reporting a “security incident”). ACNS 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, ACNS will resume coordination of the incident.

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

- Leaving affected systems on and attached to the network 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

ACNS 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.

ACNS 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

No Michigan or federal law prescribes when the University must give notice of a data system security breach to individuals whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person in connection with that data system security breach. In other states, institutions usually meet statutory notice requirements by implementation of a notice policy that is consistent with the timing requirements of the statute. The following guidelines serve as the University’s notice policy.

Deciding Whether to Notify Affected Persons

When a data system security breach that may involve the acquisition of personal information by an unauthorized person is detected, 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.

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:

- Social security number;
- Driver's license number;
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to a person's financial account;
- Student PIN (Personal Identification Number) or PAN (Personal Access Number); or
- Employee PIN or password.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Reasonable Belief of Acquisition

Existing notification laws do not provide criteria for the "reasonable belief" standard. In determining whether unencrypted personal information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person, 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 acquisition of personal information (e.g., storage and distribution of large data files)?
7. What is the likelihood that notification would unduly increase the risk of misuse of personal information?
8. What is the likelihood that the intruder has obtained data in a usable format?

Depending on the circumstances, other criteria also may be considered (e.g., potential damage to persons whose personal information may be at risk, ease of notification).

Notice

In the event that University administrators determine that notice of a data system security breach to potentially affected persons is warranted, the following procedures will be used.

- a. Notice will be given in writing, by U.S. mail, and without unreasonable delay after detection of the breach.
- b. If the cost of giving written notice is excessive, or if there is insufficient contact information to notify a potentially affected person in writing, the University will consider giving notice by one or more of the following methods:
 1. E-mail if the University has an e-mail address for the potentially affected person;
 2. Conspicuous posting of the notice on a University website; and/or
 3. Notice in the form of a press release to media.
- c. The department or unit 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.
- d. 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.
- e. The department(s) or unit(s) responsible for security of the data system will bear all costs associated with notification.
- f. If DPPS or another law enforcement agency determines that notification will impede a criminal investigation, University administrators will consider delaying notification until it is determined that notice will not compromise the investigation.