

UW-Madison

Information Incident Reporting Policy

Policy

UW-Madison employees, contractors and users of UW-Madison information resources must report incidents in which there is a reasonable belief that UW-Madison sensitive information may have been accessed by unauthorized persons. Reportable incidents include but are not limited to:

- loss or theft of computer systems, devices or media, where it is both reasonable to believe that sensitive information was present at the time of loss and reasonable to believe that unauthorized persons could access that information (for example, the information was not encrypted);
- unauthorized entry into offices or work areas, where it is reasonable to believe that sensitive information was accessed by unauthorized persons; or
- intrusion by malware or other unauthorized access via the network into computer systems or devices, where it is reasonable to believe that sensitive information was accessed by unauthorized persons.

Background

Unauthorized access to sensitive information can have significant detrimental effects on individuals or the institution. There are state and federal laws and regulations and various contracts that require the university to protect certain types of information from unauthorized access. Under some circumstances these rules require that unauthorized access be reported to the contractor, the source of the information or the individuals who might be adversely affected as a result of such unauthorized access. Identity theft is one of many examples of harm that can result. In order to take appropriate action to protect individuals and the institution from harm, the institution needs to be informed of incidents where there is a reasonable belief that UW-Madison sensitive information may have been accessed by unauthorized persons.

Information incident reporting was the highest priority among possible IT policies identified by the UW-Madison community during a series of IT policy forums held throughout the 2007-2008 academic year. In June of 2008 the CIO chartered an Information Incident Reporting (IReport) policy stakeholder's team to make recommendations leading to the development of policies and procedures. The team included representatives from several different UW-Madison units. The activities and recommendations of the team may be viewed at: <https://wiki.doit.wisc.edu/confluence/display/POLICY/IReport>.

Authority

This policy is issued by the UW-Madison CIO and Vice Provost for Information Technology.

Enforcement

Failure to report as required under the policy and procedures may result in loss of access to UW-Madison information resources, action under the terms of a contract up to and including termination of the contract, or disciplinary action up to and including termination of employment.

Related Documents

The glossary and attached procedures are extensions of the policy.

See: <https://wiki.doit.wisc.edu/confluence/display/POLICY/Glossary>

Definition of Sensitive Information:

See: <https://wiki.doit.wisc.edu/confluence/display/POLICY/Sensitive+Info>

Contact

Please direct questions about this policy to policy@cio.wisc.edu.

Policy ID:	IReport	Maintained by:	Office of the CIO, Policy and Planning Department
Effective:	Jun 1, 2009	Policy Revision:	Jun 5, 2009 (Rev B) (review period: two years)

Procedures

UW-Madison Information Incident Reporting Policy

These procedures are for use with the UW-Madison Information Incident Reporting Policy. Please see the [glossary](https://wiki.doit.wisc.edu/confluence/display/POLICY/Glossary) at <https://wiki.doit.wisc.edu/confluence/display/POLICY/Glossary>. For further background see <https://wiki.doit.wisc.edu/confluence/display/POLICY/IReport+Recommendations>.

I. Information Incident Reporting Procedure:

Whenever an UW-Madison employee, contractor or user of UW-Madison IT resources has a reasonable belief that UW-Madison sensitive information may have been accessed by unauthorized persons, the incident must be reported within no more than three working days. The earliest possible report is encouraged in order to minimize possible damage to individuals or the institution.

1. Retain evidence:

- a. In the event of theft or physical intrusion, to the extent possible do not disturb any physical evidence, and *immediately contact the UW Police Department*.
- b. Do not turn off any related computer system or device, or dispose of any related media.
- c. Do not use any related computer system, devices or media.

2. To report a possible information incident:

- a. If the incident involves theft or physical intrusion contact the UW Police Department.

Non-emergency: Call (608) 264-2677 (264-COPS)

Emergency: Dial 911 from any campus phone.

- b. In all other cases contact the DoIT Help Desk at (608) 264-4357 (264-HELP) or email to help@doit.wisc.edu. Provide as much detail as practical. DoIT Help Desk staff will log the incident and notify others according to their internal procedures.

II. Information Incident Triage Procedure (template):

In order to avoid large numbers of unnecessary information incident reports, each UW-Madison unit is encouraged to adopt or adapt this information incident triage procedure for use within the unit.

Adoption of this triage procedure template within a unit is not mandated by the policy. In the absence of procedures within a unit, those following the triage procedure template will satisfy the standard of compliance under the policy.

The information incident triage procedure is not intended to place any restriction on who may report a possible information incident.

Any UW-Madison employee, contractor or user of UW-Madison IT resources may report a possible information incident via the Information Incident Reporting Procedure.

There are three distinct triage procedures intended for different audiences:

- A. End users of the unit
- B. Local IT staff of the unit
- C. Management of the unit

A. **End users of the unit** who observe suspicious activity or events should do the following:

1. Retain evidence.

- a. In the event of theft or physical intrusion, to the extent possible do not disturb any physical evidence, and *immediately contact the UW Police Department*.
- b. Do not turn off any related computer system or device, or dispose of any related media.
- c. Do not use any related computer system, devices or media.

2. Contact local IT staff or the DoIT Help Desk.

As quickly as practical, but no later than the next business day, contact the local IT staff of the unit, or contact the DoIT Help Desk.

3. Cooperate during the subsequent investigation.

4. Done

B. **Local IT staff of the unit** who observe suspicious activity or events or receive a report from an end user should do the following:

1. Retain evidence.

- a. In the event of theft or physical intrusion, to the extent possible do not disturb any physical evidence, and *immediately contact the UW Police Department*.
- b. Do not turn off any related computer system or device, or dispose of any related media.
- c. Do not use any related computer system, devices or media except for the minimum necessary to cautiously investigate.

2. Investigate the possible information incident in a timely manner and to the extent prudent and practical.

As quickly as practical, attempt to determine to the extent prudent and practical whether or not there is a reasonable belief that UW-Madison sensitive information may have been accessed by unauthorized persons.

3. Report the possible information incident, if warranted.

If there is a reasonable belief that UW-Madison sensitive information may have been accessed by unauthorized persons, (or if it is not prudent or practical to conduct such a triage investigation in a timely manner):

a. Inform management.

As quickly as practical but no later than the next business day, contact management in accordance with unit or managerial directives.

b. Report the incident.

If management has been contacted, follow management instructions regarding the possible information incident. If management of the unit is unavailable or does not require that they be contacted, then report the possible information incident via the Information Incident Reporting Procedure as quickly as practical but no later than the next business day.

c. Cooperate during the subsequent investigation.

4. Done

C. Management of the unit who observe suspicious activity or events or receive such a report from an end user or the local IT staff should do the following:

1. Assure that evidence is retained.

- a. In the event of theft or physical intrusion, assure to the extent possible that physical evidence is undisturbed, and *immediately contact the UW Police Department*.
- b. Assure to the extent possible that any related computer system or device is not turned off, and that any related media is retained.
- c. Assure to the extent possible that any related computer system, devices or media are not used.

2. Assure that local IT staff investigate the possible information incident in a timely manner and to the extent prudent and practical.

If it has not already been done, as quickly as practical, have local IT staff attempt to determine to the extent prudent and practical whether or not there is a reasonable belief that UW-Madison sensitive information may have been accessed by unauthorized persons.

3. Assure that, if warranted, the possible information incident is reported in a timely manner.

a. Assure that the incident is reported:

If there is a reasonable belief that UW-Madison sensitive information may have been accessed by unauthorized persons, (or if it is not prudent or practical to conduct a triage investigation in a timely manner,) assure that the possible information incident is reported in a timely manner via the Information Incident Reporting Procedure.

b. Cooperate during the subsequent investigation.

c. Cooperate during any follow up response to the incident.

4. Done

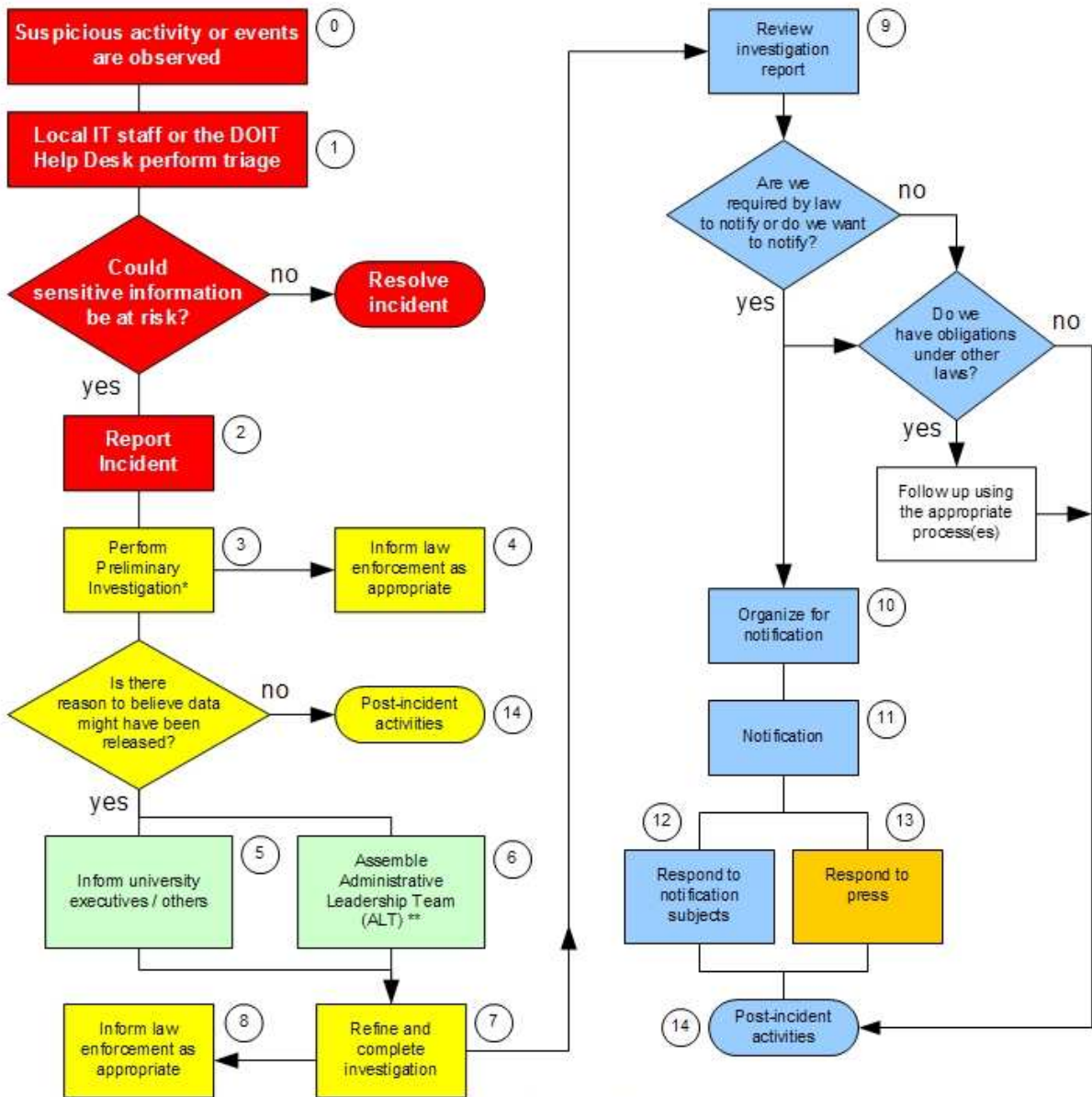
III. Recommended Training for Information Incident Reporting

Knowledge needed	End Users of the Unit	Technical Staff		Management of the Unit
		DoIT Help Desk	IT Staff of the Unit	
How to identify suspicious activity or events	Yes	Yes	Yes	Yes
How to preserve evidence	Yes	Yes	Yes	Yes
How to contact local IT staff in a timely manner	Yes			Yes
How to contact the DoIT Help Desk in a timely manner (if local IT staff are not available)	Yes			Yes
How to prudently investigate suspicious activity or events to determine whether or not there is a reasonable belief that UW-Madison sensitive information may have been accessed by unauthorized persons		Helpful	Helpful	
How to contact management of the unit regarding a possible information incident			Yes	
How to report a possible information incident in a timely manner via the Information Incident Reporting Procedure	End Users may report incidents	Yes	Yes	Management may report incidents
How to assure that a possible information incident is reported in a timely manner				Yes

UW-Madison Information Incident Reporting and Response Flowchart

Revised 01/23/2009

DRAFT



For more details at each step see:
 Information Incident Reporting and Response Process Template
<https://wiki.doit.wisc.edu/confluence/display/POLICY/IRreport+Policy/>

Who?	Department (steps 0-2)	CIO (steps 5-6)	University Communications (step 13)
	Investigator(s) * (steps 3-4, 7-8)	Administrative Leadership Team (ALT) and designees ** (steps 9-12)	

* Investigators might include: person(s) from department, OCIS, University Police, Risk Management, etc.
 ** ALT includes: CIO, OCIS, IT Policy, person(s) from department, data steward(s), legal, communications, IRB, etc.

Copyright (C) 2009 University of Wisconsin Board of Regents

L

Policy ID: IReport Maintained by: Office of the CIO, Policy and Planning Department
 Effective: Jun 1, 2009 Procedure Revision: Jun 5, 2009 (review period: one year, or sooner as needed)

UW-Madison Sensitive Information Definition

In addition to the information identified below, there are times when a data field is not considered sensitive when used alone but may be so when paired with other data. An example is date of birth. Date of birth is not considered sensitive when it stands alone but if it is available along with social security number and name it is considered sensitive.

Sensitive information may be subject to disclosure under certain circumstances. The University appropriately seeks to maintain systems that restrict access to sensitive information as defined to meet a variety of goals related to protection of sensitive information.

The data types listed below are those identified as of 5/19/2009

Sensitive Information means:

(i) Institutional Data that could, by itself or in combination with other such Data, be used for identity theft, fraud, or other such crimes. It includes Data defined as Restricted Data.¹

Restricted Data:

- Social security numbers
- Driver's license numbers and state resident/personal identification numbers
- Financial account number (including credit/debit card) or any security code, access code or password that would permit access to an individual's financial account
- Deoxyribonucleic acid profile, as defined in WI S. 939.74(2d)(a)
- Unique biometric data, including fingerprint, voice print, retina or iris image or any other unique physical representation
- Protected health information (any information about the health status, provision of health care, or payment for health care) (except workman's comp)

Other Data Types:

- Bank account numbers, automated clearinghouse and electronic funds transfer account numbers, brokerage account numbers, and other financial account numbers
- Passport numbers and alien registration numbers
- Employee and student identification numbers
- Health insurance identification numbers provided by insurance carriers
- Digital keys and passcodes
- Passwords, security codes, access codes, biometric codes, personal identification numbers, and other unique account identifiers
- Personal information such as date of birth and mother's maiden name
- Digital signatures (ink signatures that have been digitized)
- Military ID
- Garnishments, tax levies, wage assignments
- Beneficiaries, retirement account allocations and investments

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

Data Types:

- Student educational records
- Information in a person's medical record
- Human subjects research information, if the subjects have been promised anonymity
- Trade secrets or other proprietary business information owned by a third party and provided to the University upon a promise of confidentiality for the conduct of research, testing, or training, or in connection with a potential investment or transfer of technology by the University
- Proprietary computer applications or source code to which the University holds a license that restricts further or public distribution
- Exam questions and answers/scoring keys until distributed by the professor
- Bids and proposals until they are opened or the deadline for their submission has passed

- Employment data such as retirement account allocations and investments and designations of beneficiaries
- Employee home address where an employee has asked it not be released
- Documentation of grievance, arbitration, and disciplinary proceedings
- Information about pending research misconduct proceedings
- Financial aid applications and related tax and financial information
- Information and records protected by the attorney-client privilege
- Law enforcement investigation records
- Private financial data, and other information disclosed under the University's conflict of interest policies
- Information from a consumer report
- Information derived from servicing or collecting loans from, or accounts payable to, the University
- Data related to those sensitive knowledge, technologies, equipment, software, biological agents or related services that are subject to United States Government export controls

(iii) records of the University's security measures,

Data Types:

- Passwords for access to University facilities or computer systems
- 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

and (iv) Institutional Data whose value 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.

Data Types:

- 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 (like real property appraisals)
- Computer applications to which the University owns the code

Please direct questions about this document to policy@cio.wisc.edu.²

Maintained by: Office of the CIO, Policy and Planning Department
Effective: January 8, 2009

¹ Restricted Data includes information with Personal Identifying Information (PII) as specified in Wisconsin's data Breach Notification Law (statute Section 134.98). More information on data handling can be found at <http://www.cio.wisc.edu/security/uwdata.aspx#restricted>.

² The definitions in this document are directly derived from work done at the Michigan State University. Our thanks to them for allowing us to use their work.