

UW-Madison Policy for Storage and Encryption of Sensitive Information

Policy

1. UW-Madison employees and contractors must have permission from their supervisor or other appropriate authority in order to store sensitive information on desktops, laptops or other portable devices or media.
2. The presence of sensitive information on desktops, laptops and other portable devices and media must be limited to the amount necessary for immediate operations.
3. UW-Madison employees and contractors must encrypt sensitive information that is stored on desktops, laptops or other portable devices or media according to the current compliance standards.
4. UW-Madison employees and contractors must assure that encrypted information is accessible and retrievable as needed for operations and records retention purposes.

The compliance standards describe currently available resources and procedures. The compliance standards will change over time as technology and business needs change.

Background

Unauthorized access to sensitive information can have significant detrimental effects on individuals or the institution. There have been instances over the last several years of sizeable information security breaches at higher education institutions that resulted from the loss or theft of laptops or other portable devices and media. Desktop computers and devices also pose a significant risk due to the difficulty of providing adequate and consistent physical and network security. Overall, loss, theft and unauthorized physical or network access account for approximately two thirds of information security breaches.

Experience in higher education has demonstrated that a sizeable information security breach can be very costly to individuals and the institution. Anti-virus software, security updates and firewalls cannot fully protect computers and media from loss, theft and unauthorized physical access. The most effective way to reduce risk is to reduce the amount of sensitive information that is present on the more vulnerable devices and media. Encryption significantly reduces the risk of unauthorized access to any remaining sensitive information.

In June of 2008 the CIO chartered a Protection of Sensitive Information by Encryption (IEncrypt) 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/IEncrypt>.

Authority

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

Enforcement

Failure to comply may result in disciplinary action up to and including termination of employment.

Related Documents

The [glossary](#) and attached compliance standards 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:	IEncrypt	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)

Compliance Standards

UW-Madison Policy for Storage and Encryption of Sensitive Information

Please see the glossary at: <https://wiki.doit.wisc.edu/confluence/display/POLICY/Glossary>.

Sensitive information is defined at: <https://wiki.doit.wisc.edu/confluence/display/POLICY/Sensitive+Info>.

For further background see: <https://wiki.doit.wisc.edu/confluence/display/POLICY/IEncrypt+Recommendations>.

I. Suggested Implementation Procedure

A. As soon as possible:

1. Discover and review what sensitive information you have on laptops and other portable devices and media.
2. Get as much sensitive information off of those devices as possible. This could include deleting extra copies or moving the data to a secure server. Management should decide what sensitive information must remain on such devices in order to support immediate operational needs.
3. Use encryption to protect any remaining sensitive information on laptops and other portable devices and media. An institutionally managed encryption solution is available for PC's. Contact: Allen Monette, amonette@wisc.edu.

B. As soon as practical: repeat the above steps for desktop devices.

II. Requirements

A. Deadlines:

1. The compliance deadline for laptops and other portable devices and media is as soon as possible but no later than [TBD].
2. The compliance deadline for desktop devices is as soon as practical but no later than [TBD].

B. Accessibility and Retrieveability of Records:

A university approved method of key recovery must be used whenever university records are encrypted. The institutionally managed encryption solutions will employ approved methods of key recovery. If another encryption solution or method of key recovery is used, the method of key recovery must be reviewed.

C. General Exceptions:

1. Conflicts with laws, regulations or contracts.

The sensitive information must be protected with compensating controls.

When there is a conflict that apparently precludes encryption, the data steward should seek expert advice as to whether or not encryption may still be used with appropriate safeguards.

Those claiming this exemption may be asked to cite the specific law, regulation or contract.

2. Portable read only media that was written prior to the effective date of the policy.

The media must be protected with compensating controls.

Unencrypted copies of sensitive information on read only media should be destroyed if they are no longer needed, otherwise they should be replaced in the normal course of business.

3. Devices or media do not support encryption.

The device must be protected with compensating controls.

Devices that do not support encryption should be replaced as soon as practical with more modern or sophisticated devices that support encryption.

4. Operational needs of the unit. The unit determines that encryption is not operationally practical for a specific use of specific sensitive information.

The sensitive information must be protected by compensating controls.

Those claiming this exemption may be asked to provide a reasonable explanation. When encryption is deemed to be impractical due to operational need, the data stewards and data custodians should attempt to adjust procedures so that the information no longer requires encryption, or the operational impact of encryption is reduced.

5. Decisions of the data stewards. The data stewards determine that encryption is not operationally practical for a specific use of specific sensitive information.

The sensitive information must be protected by compensating controls.

6. Backups. Backups may be stored in unencrypted form.

Unencrypted backups must be protected by compensating controls.

7. The only sensitive information present is the custodian's personal information.

The custodian has the option of encrypting the information for her or his own protection, but is not required to do so.

III Recommendations

A. Encryption of sensitive information on servers:

Sensitive information on servers is not covered by this policy. Encryption should be employed as practical when sensitive information is stored on servers.

B. Encryption of transmitted information:

Transmission of sensitive information is not covered under this policy. Some form of encryption or secure network connection should be used when sensitive information is transmitted over unsecured networks. There are some types of sensitive information for which encryption during transmission is required by law, regulation, contract or policy.

C. Non-electronic media:

Non-electronic media are not covered under this policy. Adequate security controls should be implemented to protect sensitive information on such media.

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.ⁱ

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.ⁱⁱ

Maintained by: Office of the CIO, Policy and Planning Department

Effective: January 8, 2009

ⁱ 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>.

ⁱⁱ 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.