UW-Madison Policy for

Restricted Data Management

Policy

The Restricted Data Management policy will initially only apply to UW-Madison Social Security Numbers (SSN's) during the period from January 1st 2015 through December 31st 2015. The initial period may be extended. The policy will eventually apply to all UW-Madison Restricted Data.

"Restricted Data" (defined in the "Sensitive Information Definition.") includes six different kinds of data, one of which is Social Security Number (SSN). "UW-Madison Restricted Data" is Restricted Data for which the institution has an ownership, stewardship or custodial interest. It does not include data which is unrelated to UW-Madison business.

1. All Schools, Colleges, Divisions, Departments, Centers and other units of UW-Madison must at least annually find, reduce, protect, and report the storage locations of UW-Madison Restricted Data related to the unit's business, including Restricted Data stored by contractors or other entities or persons associated with the unit.

    a. Find UW-Madison Restricted Data on all computing devices and services that are used for UW-Madison business, including Restricted Data on personally-owned devices and privately contracted services when the device or service is used for UW-Madison business.

    b. Dispose of unneeded files, data records, or data sets that contain UW-Madison Restricted Data, being careful to retain UW-Madison records according to the approved records retention schedules.

    c. Move as many of the remaining instances of UW-Madison Restricted Data as practical into any of the offline or online storage locations that are approved by UW-Madison IT Security for the long-term storage of Restricted Data, retaining in other locations only those instances that are necessary for immediate operations.

    d. Report all remaining instances of UW-Madison Restricted Data to UW-Madison IT Security using the currently established reporting procedures.

2. Accountability and responsibility for compliance with provision (1) of the policy is distributed as follows:

    a. Management for each School, College, Division, Department, Center or other unit of UW-Madison is accountable to higher management for the compliance of their unit, including all employees, contractors and associates.

    b. Employees, contractors and associates of each unit are responsible for making computing devices and services that they own, operate, or possess available for inspection if that device or service is used for UW-Madison business.

    Some UW-Madison Restricted Data is stored on personally-owned devices or privately contracted services that are being used for UW-Madison business. UW-Madison is obligated to assure that UW-Madison Restricted Data is appropriately protected, regardless of the ownership or location of the device or service.

    The university respects the privacy of individuals and non-university entities. As an alternative to inspection, employees, contractors and associates may provide satisfactory assurances that either:

        i. there is not significant storage or use of UW-Madison Restricted Data on the device or service.
        ii. if there is significant storage or use, either:
            a. the storage or use will be reduced in a timely manner so it is no longer significant, or
            b. the device or service is, or soon will be, protected as described by the mandatory portions of the applicable data security standard.

The threshold for "significant use" is specified in the associated implementation procedures.

Management for each unit determines what assurances are satisfactory, consistent with the guidelines provided in the associated implementation procedures, subject to review by higher management in consultation with UW-Madison IT Security.

c. Responsibility for providing technical or procedural support may be delegated to IT staff, but this does not relieve others from their accountability and responsibility as described in (2)(a-b).

3. UW-Madison data stewards, data custodians, business process owners and others with similar responsibilities for managing data must, when practical, eliminate or reduce the presence of UW-Madison Restricted Data in forms, files, data records, data sets, databases, applications, processes, and other similar locations.

4. The Restricted Data Management policy and the associated implementation procedures provide general criteria for managing UW-Madison Restricted Data. When more specific guidance is needed, the data stewards or their delegates, in consultation with UW-Madison IT Security, make the final decision on the conditions under which UW-Madison Restricted Data may be present in particular circumstances.

Special cases

1. The Restricted Data Management policy applies to all computing devices and services that are used for UW-Madison business, regardless of who owns, operates, or possesses them, including both UW-Madison-owned and non-UW-Madison-owned devices and services. The associated implementation procedures provide guidance on how to address personally-owned devices and privately contracted services in a manner that respects the privacy of individuals and non-university entities.

2. This policy applies to graduate and undergraduate student employees in the performance of their job duties. Students are otherwise exempt from this policy.

3. Exceptions are described in the associated implementation procedures.

Background

The long-term purpose of the Restricted Data Management policy is to identify and appropriately manage all UW-Madison Restricted Data.

In order to identify and manage the highest risk data as quickly as practical, the Restricted Data Management policy will initially only apply to UW-Madison SSN's during the period from January 1st 2015 through December 31st 2015. The initial period may be extended. The policy will eventually apply to all UW-Madison Restricted Data.

Unauthorized access to Restricted Data can have significant detrimental effects on individuals or the institution. Restricted Data can be used for fraud and identity theft. Cyber criminals regularly attack computers and networks in higher education institutions. There have been sizeable information security breaches at institutions that resulted in financial impacts of many hundreds of thousands dollars. Those amounts do not account for the loss of reputation and trust that can have a serious ongoing impact on both instruction and research.

The university is obligated to protect UW-Madison Restricted Data and to report possible incidents. Protection of Restricted Data is governed by a number of different laws and standards, including for example, the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI-DSS), and the Wisconsin Data Breach Notification Law.

In order to protect Restricted Data the institution must have up-to-date information about where it is stored. There is a significant reduction in risk if the presence of Restricted Data is reduced to the extent practical. In addition to finding and reporting the presence of the data, the annual discovery and reporting process is a convenient time to consider how the presence of the data can be reduced.

The university's obligation to protect UW-Madison Restricted Data does not depend upon the location or ownership of the computing device or service which is used to store, transmit or process it. For this reason, the policy and procedures address both UW-Madison-owned and non-UW-Madison-owned computing devices and services that are used for UW-Madison business.

The university respects the privacy of employees, contractors, and associates. The university is obligated to appropriately manage all UW-Madison data no matter how it is stored, transmitted, or processed. The policy and associated implementation procedures include provisions that protect privacy while at the same time enabling the institution to fulfill its obligations.

Authority

This policy is issued by the Vice Provost for Information Technology.

Enforcement

Failure to comply may result in appropriate action to enforce compliance, and/or denial of access to UW-Madison Restricted Data or other UW-Madison information resources. In addition:

1. UW-Madison employees who do not comply may be subject to disciplinary action up to and including termination of employment.
2. Contractors or associates who do not comply may be subject to penalty under the governing agreement. Compliance with the policy may be a consideration affecting new or renewed agreements.
3. Computing services or devices may be denied access to UW-Madison information resources to assure that UW-Madison Restricted Data is only present in known locations that are adequately protected.

Contact

Please address questions or comments about this policy to policy@cio.wisc.edu.

Related Documents

The "IT Policy Glossary" defines a number of terms used in this policy.

The appropriate protection for UW-Madison SSN's is defined by the UW-Madison Departmental IT Security Baseline plus the CIO IT policies that apply to Sensitive Information.

The DoIT Knowledge Base (KB) has a document on Getting Started with Identity Finder, which includes training and links to other KB articles. There is also an Identify Finder FAQ, and a list of all related articles.

The mandatory portions of the associated implementation procedures have the same authority as this policy.

There are numerous other policies that govern the protection of UW-Madison Restricted Data. These may vary according to the specific type of Restricted Data, or how that data is collected or used.

RDM Policy | Review: in one year | Published at: http://www.cio.wisc.edu/policies/
Effective: Jan 1, 2015 | Reviewed: Apr 14, 2015 | Maintained by: Office of the CIO, IT Policy Office
Revised: Apr 14, 2015 | For history see: https://wiki.doit.wisc.edu/confluence/display/POLICY/DataDiscovery

Implementation Procedures
UW-Madison Policy for Restricted Data Management

1. Initial emphasis on UW-Madison Social Security Numbers (SSN's)

a. During the initial period from January 1st 2015 through December 31st 2015 the Restricted Data Management policy will only apply to UW-Madison SSN's. The initial period may be extended. For clarity and simplicity, the implementation procedures and other supporting documentation will initially be written to address only SSN's.

b. A threshold value of "more than 100 unique UW-Madison SSN's" indicates there is significant use that requires action at an increased priority level to locate and protect the data. A UW-Madison unit may choose to use a lower threshold value. A higher threshold value may be used with the consent of the leadership of the unit and UW-Madison IT Security.

2. Priorities for discovery of UW-Madison SSN's

a. **At high priority,** (i.e. higher than "routine administrative operations,") check UW-Madison-owned or -operated systems where data on the system can be scanned with Identify Finder and:

i. At least one user of a desktop or laptop system is a person whose role at the institution has made them a direct user of the Integrated Student Information System (ISIS), the Shared Financial System (SFS), the Human Resource System (HRS), or the UW-Madison data warehouse (InfoAccess).

Scanning of enterprise systems has shown that the vast majority of UW-Madison SSN's are located in one of those four systems. The direct users of those systems are likely to have SSN's.

For assistance identifying those users contact: restricteddata@doit.wisc.edu.

ii. At least one user of a desktop or laptop system is a person who has been a recipient of data or reports from the direct users of ISIS, SFS, HRS, or InfoAccess.

Many direct users of these enterprise system are providing data or sending reports to others. The recipients are also likely to have SSN's.

To identify those users:

- People who have sent reports to others may be able to identify who received them.
- Those who have received reports may be able to self-identify.

iii. On a server, check areas used for data storage by users identified in (i) and (ii) above, unless the only use of the server by those users fits one of the exceptions listed in procedure (7) .

Rather than attempting to narrow the area scanned, it might be simpler to scan an entire server. It might be simpler to scan all servers that could contain data from such users.

All checks done at high priority involve UW-Madison-owned or -operated systems where the data can be scanned with Identify Finder. Use of Identity Finder is not required. When using Identity Finder, if Identity Finder cannot be run on a system, it may be possible to make the data accessible to a system on which Identity Finder can be run. For more information see the list of all KB articles related to Identity Finder.

b. **At moderate priority** (i.e. similar to "routine administrative operations,") check:

i. Desktops, laptops, portable devices, cloud services, or other data storage locations that are used by a person for whom Identity Finder scans (or manual checks) described in (2)(a) above have discovered more than 100 unique UW-Madison SSN's associated with that person's server, desktop, or laptop use.

Some checking may need to be done manually either by:

1) examining the device, service or other storage location, or

2) interviewing the user to determine what UW-Madison SSN's (if any) might be present in such locations.

ii. Other storage locations of any kind where the pattern of usage or other prior experience make it reasonable to believe that there may be more than 100 unique UW-Madison SSN's present.

Some checks done at moderate priority may involve personally owned devices or privately contracted services that are used for UW-Madison business. See procedure (6) below for how to handle this in a manner that respects the privacy of individuals.

c. **At low priority,** as workload or circumstances allow, check other storage locations that are used for UW-Madison business, unless the only use of the location fits one of the exceptions listed in procedure (7) below. See procedure (6) below for how handle personally owned-devices or privately contracted services in a manner that respects the privacy of individuals and non-university entities.

   There are several hundred thousand locations where a UW-Madison SSN might be located. It is not practical to check every one of them. Priority should be placed on high and moderate risk locations such as those described in (2)(a-b) above. Nevertheless, other plausible locations should be scanned or manually checked when it is practical to do so.

3. Annual discovery and reporting of UW-Madison SSN's

Provisions (1)(a) and (1)(d) of the policy mandate the annual discovery and reporting of the presence of UW-Madison SSN's. Details for reporting are published in the DoIT Knowledge Base (KB).

The use of Identity Finder is recommended, but is not required by the policy. The recommended configuration of Identity Finder will be tuned to find SSN's while minimizing the number of false positives. There will inevitably be some false positives. For more information see the list of all KB articles related to Identity Finder.

The annual discovery and reporting process does not preclude checking systems more frequently. Results from checks that are less than one year old can be used when preparing the annual report.

When Identity Finder is not used:

a. If it is *reasonable to believe that UW-Madison SSN's are present*, the storage location must be reported as a location that contains UW-Madison SSN's.

   For example, an analysis of business processes might indicate that a device or service is likely to contain SSN's. It is not necessary to confirm that SSN's are present. Simply report the device or service as a location that contains SSN's.

   There is no practical distinction between the likely presence and the confirmed presence of UW-Madison SSN's. Either way, the storage location needs to be managed as one that contains UW-Madison SSN's.

b. If it is *reasonable to believe that UW-Madison SSN's are not present*, that storage location need not be reported as a location that contains UW-Madison SSN's.

   For example, an analysis of the pattern of usage might indicate that it is unlikely that UW-Madison SSN's are present. A report of this is not required. The intent of the reporting requirement is to locate UW-Madison SSN's. It is not the intent to create an inventory of all storage location.

   There is no practical distinction between a location that is unlikely to contain UW-Madison SSN's and one where the absence of SSN's has been confirmed. Either way, the location need not be managed as one that contains UW-Madison SSN's.

   Exercise caution when deciding that a computing device or service is unlikely to contain SSN's. People often do not realize SSN's are present. UW-Madison employee and student ID numbers previously included the same digits as the person's SSN. Research proposals prior to 2006 sometimes required the SSN's of the collaborators. Certain UW-Madison business processes currently require the use of SSN's. Email is particularly prone to contain unexpected or forgotten collections of SSN's.

c. If neither (a) nor (b) applies, the presence or absence of UW-Madison SSN's is considered sufficiently uncertain to warrant reporting the storage location as a location that contains UW-Madison SSN's. The degree of protection required is uncertain, but some additional protection may be warranted, depending upon the circumstances.

   Example reasons why a location may be a possible location of UW-Madison SSN's include:

   - An analysis of business processes or patterns of usage is unable to determine that it is likely or unlikely that SSN's are present.

- It is not practical to scan the location using Identity Finder, and the data in that location is too large, complex or otherwise difficult to evaluate using other methods.
- It is not practical to inspect or assure that a device or service does not contain or process a significant number of SSN's.

d. When the presence of encrypted UW-Madison SSN's is known, likely or suspected, the location must be reported as one that contains UW-Madison SSN's.

While encrypted data is generally more secure than unencrypted data, encryption does not provide protection against attacks that can access the data when it is presented to the user or application in decrypted form. This is not an unusual scenario, because data can only be viewed or changed while decrypted.

For example, "full disk" encryption of a laptop or other computing device usually requires entering the password or other key when the device is *started*. While the data on the physical storage media remains encrypted, the data is automatically presented to the operating system and applications in decrypted form. Any attack that compromises the *running* device will evade the encryption.

While encrypted, it might not be possible or practical to use Identify Finder or other checks to locate UW-Madison SSN's within the data. This will depend upon how the data is encrypted. In such cases, it may still be possible to deduce that UW-Madison SSN's are likely or possibly present, based upon the type or use of the data.

4. Reducing the Presence of UW Madison SSN's

Provisions (1)(b), (1)(c) and (3) of the policy require that the presence of UW-Madison SSN's be reduced to the extent practical. What is practical to accomplish is a question of professional judgment guided by appropriate risk management.

The requirements for discovery and reporting of SSN's are distinct from the requirements to reduce the presence of SSN's. The people responsible for finding SSN's are not necessarily the same people responsible for reducing their presence. If SSN's are discovered by someone who is unable to reduce their presence, the recommended course of action is to simply report the location of the SSN's as described in procedure (3). UW-Madison IT Security will follow up and work with people to help them reduce the presence of SSN's.

The following are examples of ways to reduce the presence of UW-Madison SSN's:

a. During the annual discovery and reporting process, instances of SSN's may be found that are no longer needed for immediate operations. (See provisions (1)(b) and (1)(c) of the policy.) When this occurs:

i. Some instances of SSN's may be disposed of. Examples include SSN's that are not part of a UW-Madison record, or are included in other data that is not needed for future operations.

Whenever possible, disposal is the preferred approach. Be careful to retain UW-Madison records according to the approved records management schedule. The Common Records Guide at http://archives.library.wisc.edu/records/handouts/crecsguide.pdf may be helpful. Please note that the document does not cover all cases.

If you have questions about UW-Madison records or record retention schedules, please contact Records Management at http://archives.library.wisc.edu/records/contact-recmngt.html.

ii. Some instances of SSN's must be retained. Examples include SSN's that are part of a UW-Madison record, or are part of data that is needed for future operations.

When retaining SSN's, the preferred approach is to move the data to any offline or online storage location that is approved by UW-Madison IT Security for the long-term storage of UW-Madison SSN's.

Only the minimum number of UW-Madison SSN's necessary for immediate operations should be retained in other storage locations. How much to retain is a matter of professional judgment guided by appropriate risk management.

Approved locations for the long-term storage of UW-Madison SSN's will be published in the KB as they become available. To get started:

- Offline storage of media in a locked cabinet or other physically secure area is acceptable.
- Strong encryption of the data is acceptable. For guidelines, see the "Draft Recommended Procedures for Faculty, Staff and Student Employees" at IEncrypt Policy Drafts.
- There are approved storage locations in the UW-Madison Data Center. For more information contact Enterprise Storage at: https://www.doit.wisc.edu/storage/contact-us/.
- Any location that is substantially compliant with the following standards is approved for the long-term storage of UW-Madison SSN's:
    - The Payment Card Industry Data Security Standard (PCI-DSS)
    - The Health Insurance Portability and Accountability Act Security Standard (HIPAA Security Standard)
    - The Federal Information Security Management Act (FISMA) implementing the moderate or higher security controls documented in the most recent revision of the National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) and related publications.
    - A variety of other security standards used in other locations where UW-Madison SSN's might be stored. For more information contact UW-Madison IT Security.

b. There are opportunities to reduce the presence of UW-Madison SSN's in forms, files, data records, data sets, databases, applications, processes, and other similar storage locations. The data stewards, data custodians, process owners, and others with similar data management responsibilities are responsible for reducing the presence of UW-Madison SSN's to the extent practical. (See provision (3) of the policy.) Examples of ways to accomplish this include:

- SSN might no longer be needed. Use of SSN was more prevalent in the past.
- Use a partial identifier such as the last for digits of SSN.
- Use a different identifier such as student or employee id. When the SSN is needed, use a separate and secure data service to lookup the person's SSN.

5. Protecting SSN's that are not in locations approved for the long-term storage of UW-Madison SSN's.

It is usually necessary to apply appropriate security controls when more than 100 unique UW-Madison SSN's are present in a location that is not approved for the long-term storage of UW-Madison SSN's. These controls are currently specified in the UW-Madison Departmental IT Security Baseline and the CIO IT policies that apply to sensitive information. If some of the specified controls are impractical, other compensating controls may be applied.

The policy does not mandate that the Departmental IT Security Baseline be followed in its entirety. Like most standards, some parts are mandatory and other parts are recommended.

Some of the controls in the Departmental IT Security Baseline are mandated by other policies published at http://www.cio.wisc.edu/policies/. Examples include:

Responsible Use	IT Compliance Agreement
Electronic Devices	Information Incident Reporting
Password Standard	Storage and Encryption of Sensitive Information

Having 100 or fewer unique UW-Madison SSN's does not exempt a location from other policy requirements. The threshold value of "more than 100 unique UW-Madison SSN's" indicates that security controls of all kinds need to be applied at higher priority.

6. Discovery and reporting for personally-owned devices or privately contracted services

The policy applies to personally-owned devices or privately contracted services that are used for UW-Madison business. Both university and non-university data may be mixed together in such locations.

Business use of personally-owned devices or privately contracted services

UW-Madison employees, contractors and associates who are required to use or choose to use their own devices or contracted services for UW-Madison business are obligated to either:

a. allow the device or service to be inspected, or

b. provide satisfactory assurances that either:

   i. there are 100 or fewer unique UW-Madison SSN's present on the device or service, or

   ii. if more than 100 are present, either:

   - the number of unique UW-Madison SSN's present will be reduced in a timely manner to 100 or fewer, or
   - the UW-Madison SSN's are or soon will be protected as described in the mandatory portions of the UW-Madison Departmental IT Security Baseline and the CIO IT policies that apply to sensitive information, or if not protected in that manner, other compensating security controls will be implemented in a timely manner.

The university respects the privacy of employees, contractors and associates. Attempting to force an inspection of non-UW-Madison owned computing devices or services is inconsistent with respect for the privacy of the individual or non-university entity. The option to provide satisfactory assurances respects their privacy while at the same time allowing the UW-Madison to meet its obligations to locate and protect UW-Madison data.

Satisfactory assurances

Assurances are satisfactory if a reasonable person would perceive them as satisfactory. Management of the unit is accountable for compliance, and will determine what is sufficiently satisfactory. This may vary with the circumstances.

Satisfactory assurances do not need to be onerous or invasive. For example, a simple oral assurance that 100 or fewer UW-Madison SSN's are present may be satisfactory when typical patterns of use indicate that under normal circumstances few SSN's should be present. When it seems likely that more are present, the owner might be asked to check some typical locations, and if any are found, delete unneeded copies of the data. Other criteria are possible, depending on the circumstances.

As warranted, higher management, in consultation with UW-Madison IT Security, can provide additional guidance to clarify what is considered satisfactory.

If there is significant ongoing uncertainty regarding the presence of 100 or more unique UW-Madison SSN's, the preferred course of action is to report the device or service as a location that contains UW-Madison SSN's. See procedure (3)(c) above. Uncertainty increases risk. If the risk appears to be too high, the university may follow up to find ways to reduce the risk.

7. Exceptions and Exception Procedures

a. It is not necessary to scan, manually check, or report a storage location if:

   i. the location is a device or service that only stores data temporarily and under normal circumstances will automatically delete it after some reasonably short period of time, for example: printers, copiers, scanners, network devices, and other similar devices or services.

   ii. the only SSN's that are present or likely to be present are the result of personal di minimis use (as permitted by the Responsible Use Policy.) Users are responsible for exercising discretion in where they store such SSN's.

   iii. the only UW-Madison SSN that is likely to be present is the user's own SSN. The user is responsible for exercising discretion in where and how they store their own SSN.

iv. it is otherwise reasonable to believe that UW-Madison SSN's are not present at the location.

Be cautious in making an exception for this reason. Experience over the last few years has shown that people tend to underestimate the presence of SSN's.

- Email and email attachments tend to be an unexpected location of SSN's. The sender or receiver may not realize or remember that SSN's are present.
- Some current UW-Madison business processes require use of SSN. It is not unusual for this to result in the retention of SSN's. This is is easy to overlook or forget.
- Other likely locations include instructional, research and financial data or reports created prior to 2006. SSN was more widely used as a personal identifier in past. Large numbers of SSN's (more than 100) can be unexpectedly present in older data.

b. Circumstances may warrant other exceptions. Please contact UW-Madison IT Security regarding other possible exceptions. Please see the contact information in (9) below.

8. Additional procedures

a. UW-Madison IT Security will publish additional procedures in the DoIT Knowledge Base (KB).

b. If what you need is not present in the KB, please contact UW-Madison IT Security.

9. Contact

Please direct questions or comments on these procedures to UW-Madison IT Security by emailing restricteddata@doit.wisc.edu or by using the contact forms at http://www.cio.wisc.edu/security.

For assistance identifying users of ISIS, SFS, HRS or InfoAccess, please contact: restricteddata@doit.wisc.edu

For UW-Madison SSN storage options in the UW-Madison Data Center, please contact Enterprise Storage at: https://www.doit.wisc.edu/services/file-storage/.

For questions about UW-Madison records or records retention schedules please contact Records Management at: http://archives.library.wisc.edu/records/contact-recmngt.html.

10. References

CIO IT Policies
Common Records Guide
Departmental IT Security Baseline
Electronic Devices
Getting Started with Identity Finder
Identify Finder FAQ
IT Compliance Agreement
Information Incident Reporting
List of all Identity Finder articles
Password Standard
Responsible Use
Storage and Encryption of Sensitive Information

