Guide to Appropriate Use of Social Security Numbers

MAY 27, 2010

Version 1.0

UNIVERSITY of WASHINGTON

Table of Contents

Acknowledgements

This guide was developed by the Institutional Practices, Systems/Technology and Education and Awareness Sub-teams of the Social Security Number Data Security Project Initiative.

The Institutional Practices Sub-team members are: Cindy Gregovich (Leader), Ann Nagel, Karen Low, Joseph Kittleson, Curtis Colvin.

The Systems/Technology Sub-team members are: Bill Shirey (Leader), Cindy Gregovich, Nathan Dors, Joseph Kittleson, Scott Hansen, Brad Greer, Marcus Hirsch.

The Education and Awareness Sub-team members are: Ann Nagel (Leader), Cindy Gregovich, Karen Low, Todd Mildon, Linda R. Nelson.

Revision History

This guide is a "living" document. As the direction, guidance or standard in relation to the handling of SSN data may change over time; content may be added or changed.

If you are reading a printed version of this document, please check the latest online version stored on the **Social Security Number Data Security Framework Website**

http://f2.washington.edu/fm/payroll/ssn-dsi

to ensure that you are viewing the most current version.

Date	Version	Comments
5/27/10	1.0	Initial Release

Introduction

This guide is intended to help UW staff understand their role and responsibility in the appropriate use of Social Security Numbers (SSN). SSNs are considered confidential data according to UW Administrative Policy Statement (APS) 2.10, UW Minimum Data Security Standards.

Appropriate use of SSNs (and other confidential data) is a six-step process:

1. Understand why we care about information security
2. Understand your department's need for and use of SSNs
3. Understand where you are storing SSNs
4. Control access to SSNs
5. Protect SSNs from misuse
6. Securely remove SSNs when no longer needed

The sections of this guide will help you complete these steps. Each section contains questions you should consider at each step, best practices related to that step, and tools to help you complete the step. For ease of reference, the questions are consolidated in Appendix 2, and the best practices are consolidated in Appendix 3.

Please note that everyone who is accountable for the management of SSN data must become familiar with other university-wide and departmental policies, standards, and procedures related to records management and information security that are published separately.

Section 1: Why do we care

Overview

The University of Washington routinely collects Social Security Numbers (SSNs) in support of several federal requirements such as W-2 tax forms and student educational tax credit reporting. SSNs are considered confidential data according to the UW Administrative Policy Statement (APS) 2.10, UW Minimum Data Security Standard. Unauthorized release of SSN (and other personally-identifiable information) by the UW exposes individuals to identity theft and fraud, and brings financial and reputational harm to the UW. Furthermore, federal and state breach notification laws impose costly notification and mitigation processes on organizations that have unauthorized release of SSNs. At the UW, those costs are borne by the unit whose data is compromised. Studies have shown that the costs of notification and mitigation typically exceed $150 for each exposed SSN.

Extra care is especially important in a University setting. The relative openness of university networks is particularly appealing to the information thieves who use SSNs and other personally-identifiable information to commit identity theft and fraud. The UW's decentralized administration makes us especially vulnerable.

Foundation for information security

The UW has several policies and standards that create a foundation for information security, integrity, and availability of institutional information:

- APS 2.1 "Information Systems Security Policy"
- APS 2.4 "Information Security and Privacy Roles, Responsibilities, and Definitions"
- APS 2.5 "Information Security and Privacy Incident Management Policy"
- APS 2.X "Privacy Policy"
- APS 2.10 "Minimum Data Security Standards"
- APS 2.X "SSN Standard"

Figure 1.1 shows the interrelationships between these policies and standards. Note that individual units may have policies and standards that go beyond these.

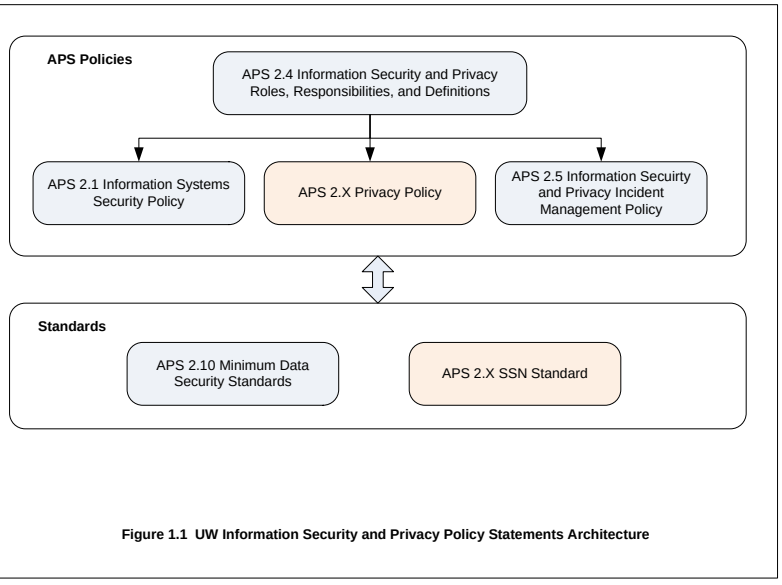


Figure 1.1 UW Information Security and Privacy Policy Statements Architecture

APS 2.4 defines roles and responsibilities related to information security. Everyone who uses institutional information is responsible for understanding their roles and responsibilities, including departmental policies and standards that go beyond the institutional policies. Figure 1.2 shows the interrelationships between the roles and responsibilities.

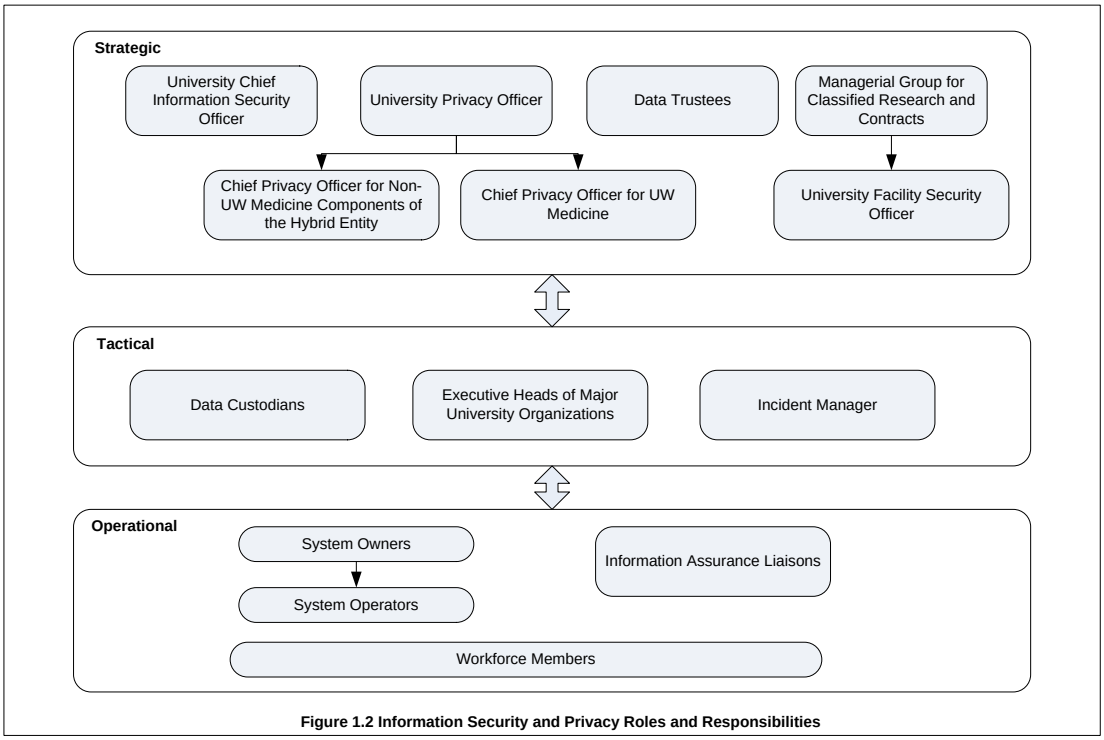


Figure 1.2 Information Security and Privacy Roles and Responsibilities

Section 2: Understanding Your Data

Overview

As noted in APS 2.X, SSN Standard, the University of Washington is obligated to collect SSN in support of several state and federal requirements such as federal tax reporting. The SSN Standard requires units to get approval from the PASS Council prior to collecting SSN for uses not identified in the SSN Standard.

If your unit collects and retains SSNs, it is important that you understand why you are collecting SSN and what additional information you are collecting with SSN. In most cases, the UW Employee Identification Number (EID) is an appropriate substitute for employee SSN.

Questions to consider

1. What are the business needs and/or legal requirements for using SSNs?

2. Is there an alternative identifier that would suffice, such as Employee ID Number (EID), UW NetID, Student Number, or other? If so, see Section 6, Data Removal, for information on how to securely remove SSN from your files.

3. What other personally identifying data elements will be used in conjunction with SSN as part of the process (e.g. name, date of birth, address, phone number, etc.)?

4. How will you inform individuals (a) whether they are legally required, or may refuse, to supply their SSN, and (b) of any consequences of providing or not providing their SSN?

Best Practices

1. Use the SSN Standard and UW and departmental policies to determine if the collection, use, storage, or disclosure of SSN is appropriate.

2. Understand the Retention Schedule for the documents which contain SSN. If the UW is not required to retain the document, securely destroy documents containing SSN as soon as possible (including paper, post-It notes, spreadsheets, microfiche, computer files, etc.) Don't keep copies of official documents which are being retained by another department (e.g. I-9 and W-4 forms should only be retained in the UW Payroll Office.)

3. If you have identified a business need for SSN, consider masking part of the number (e.g. only display the last four digits: XXX-XX-1234).

4. Be aware of disclosing sensitive information over the phone. Verify the caller. Obtain permission before leaving personal information on voice mail or answering machines.

5. Avoid asking for SSN over the phone. Is there another way to verify the identity of the caller? (EID, Student Number, address, etc).

6. Be aware of conversations involving personal information. Can the conversation be overheard?

7. Require written consent or Power of Attorney before sharing personal information such as SSN with a third party (including spouse, parent, and relatives).

8. Don't collect SSN if it is not required. Most background checks can be completed without SSN. Remove SSN from paper forms unless required.

9. Whenever possible, avoid sending documents containing SSN through campus mail; deliver in person.

10. SSNs and other sensitive information should only be FAXed to known parties where access to the FAX machine is limited and protected:

    - Notify the recipient in advance that sensitive information is being transmitted.
    - Indicate on the FAX cover sheet that the materials are confidential.
    - Confirm that the materials have been received.

Section 3: Where does it reside

Overview

If you are going to store confidential information such as Social Security Number in your department, it is important for you to understand where it resides. This applies to paper files as well as information stored in computer files and data bases. If you understand where the information is stored, you can develop appropriate access controls (see Section 4).

This Guide includes two tools to help you document where you are storing confidential data such as SSN: Inventory Worksheets and Data Flow Diagrams.

Questions to consider

1. How does the information flow? Include all points where SSNs are:
    - Solicited or collected (e.g. paper forms, web forms, or data feeds from other systems)
    - Loaded into a system
    - Used in interactions with other UW systems
    - Shared with third parties outside the UW
    - Displayed on documents, printed reports, or screens
    - Included on mailed documents
    - Transmitted over the Internet or other data connection, including FAX
    - Sent via e-mail
    - Stored in a document imaging system
    - Backed up or archived

    Completing the Inventory Worksheets and Data Flow Diagrams (see below) are an effective way to document this.

2. If the SSN will be shared with another organization (inside or outside the UW), how will it move between entities (both electronically and non-electronically)?

Best Practices

1. Complete the Inventory Worksheets and Data Flow Diagrams to assist you in making proper decisions regarding the collection, use, and disclosure of SSNs

2. Store paper containing SSNs in a secure location such as a locked file cabinet

3. Limit distribution of documents with sensitive information. How is the information maintained? Is the information exchanged?

4. All departmental application systems should be registered with the **UW Application Portfolio**, a comprehensive catalog of UW administrative applications and their functions.

Complete an SSN Inventory

Review each of your departmental business processes identifying where you:

- Solicit or collect SSNs
- Store SSNs
- Use SSN as an account number or identifier
- Use SSNs in interactions with other systems at the University
- Share SSNs with third parties outside the University
- Have archived or other "old" records that include SSNs
- Display SSNs on any documents or screens
- Include SSNs on any mailed documents
- Transmit SSNs over the Internet or through other data connections (including fax)
- Send SSNs in e-mail
- Store items with SSNs in a document imaging system

Look at the above list and note that *processes*, not just specific spreadsheets or forms, should be reviewed. For example, for a particular employee transaction in your unit, staff may collect SSNs on forms, other staff may key the information into a database, someone may review the data on screen or by printed report, the data may be shared with another unit or a reporting entity, the completed paper forms may stored in file cabinets (or a document imaging system), the database may be backed up nightly and older data may be archived to CD-ROM. The SSN use at each point must be identified in preparation for eliminating or reducing and securing its use at each point.

Templates

Appendix 1 contains several templates that may be useful for inventorying SSN use. You are encouraged to adapt these templates to your particular needs or develop other formats.

1. SSN Data Inventory Worksheet
2. SSN Documents Tracking Sheet
3. Tracking Sheet for Identified SSN Usage
4. SSN Remediation Plan

- As outlined in the UW Administrative Policy statement

  Minimum Data Security Standards: Data Classification and Related Measures of Protection
  http://www.washington.edu/admin/rules/APS/02.10.20html

  there are other types of data classified as confidential. As long as you are expending effort to review, locate, and document your department's use of SSNs you should also review the presence of other confidential data such as protected health information (HIPAA), student information (FERPA), and credit card information (PCI).

Develop a Data Flow Diagram

What is a Data Flow Diagram?

In simpest terms, Data Flow Diagrams for information systems show the movement of data from outside the system into the system, through the system including storage, and then out again. With input from both business and technical stakeholders they can be used to provide a representation of any computer system and business process. In order to create a successful DFD it is essential that business and technical stakeholders work together. When done properly through such partnership, DFDs reveal relationships among and between the various components in a system that the people who manage and use the system and its related business processes may not be aware of as individuals. Taken together and diagrammed this information is a great first step in identifying possible areas of concern for data

security and can also provide insights for other areas of improvements.
When building a data flow diagram the most basic questions are:

1. Where does the data that passes through the system come from?
2. Where does it go in the system?
3. Where does it go when it leaves?

IMPORTANT: For purposes of creating a DFD, a "System" is not limited to one computer or server or business process. It is the collection of people, business processes, hardware, and software that are associated with the data flow that is being mapped. It may be helpful to think of it as an "ecosystem" where there is a constant interaction of the constituent parts.

- It is essential that business and technical resources work together to develop the Data Flow Diagram.

Developing a Data Flow Diagram

Step #1	Technical staff create a high level map of "the system" to serve as a basis for discussion. Business stakeholders need to be ready to accept that this map may be wrong and/or incomplete. That is OK!
Step #2	Business and technical stakeholders meet to discuss the map and fill in any missing technical areas. Business interactions (such as data entry or the running of a report or emailing information taken from the system) are then added at this high level – remember, think "ecosystem".
Step #3	Business stakeholders create more detailed process DFDs for each area where they interact with "the system" including the data that is used (entered, copied to a piece of paper from the screen, viewed in a report, emailed, etc.). These are both the inputs and outputs of the system.
Step #4	Technical staff using their own system knowledge and the business stakeholders DFDs create more detailed DFDs for each area of the system. How does data move from input through the system? Where is it stored? How is it extracted? This isn't just the server or application: it includes reports, spreadsheets, file transfers and UI displays. Be sure to highlight the location and flow of confidential information such as SSN.
Step #5:	Gap analysis time! Even the best systems and business processes are likely to have areas that are disconnected, insecure, or inefficient. Working together using the DFDs, stakeholders should identify these so that they can be prioritized for resolution.
Step #6:	Start at Step #1 using the more complete DFDs now available to confirm that "the system" has been comprehensively mapped. Use the completed DFDs as a resource for prioritizing changes that will improve

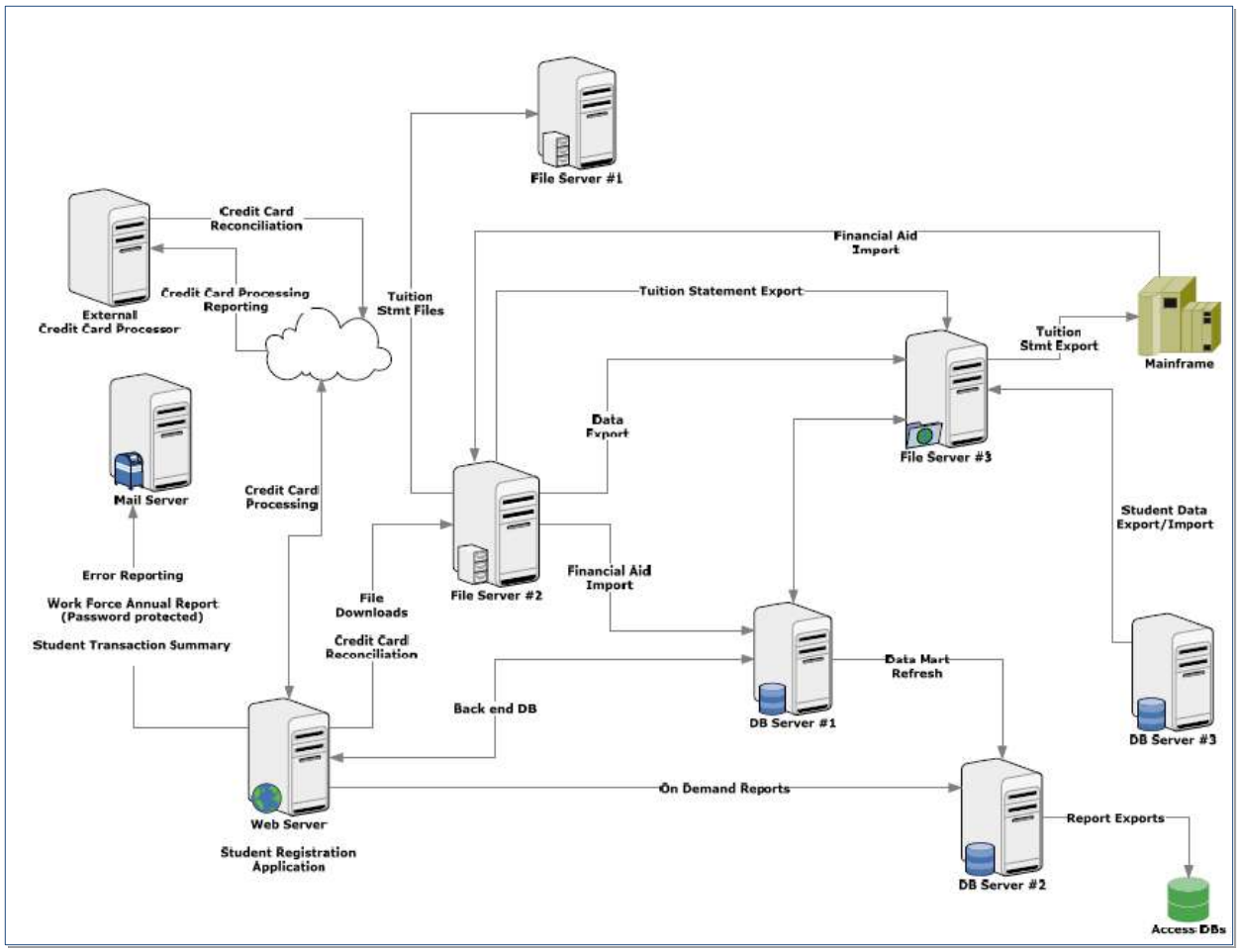
	business process, system function, and information security. As “the system” changes, remember to keep your DFDs up to date!

Data Flow Diagrams have different levels. Starting at a high level and then working down into the detailed level allows business and technical people to work together to complete a comprehensive map. Technical staff might develop a high level systems map to start the discussion such as the diagram of a sample student registration data flow below to serve as the foundation for more detailed DFDs for each portion of the process as necessary. In this example there is more detail on both the technical and business process side to understand each area.

- Business: What is the process for using the “student registration application”? What does the student enter? Why do we need that data?
- Technical: Is the web form secure? What happens to the data when the student clicks on a “submit” or “register” button? How does the data get to and from DB Server #1? Each of these questions might lead to an additional small map depending on the level of detail desired.

■ **Learn more: There are many resources online and in applications like Microsoft’s Visio or Oracle’s Open Office Draw that will help you learn to create DFDs.**

Example Data Flow Diagram:



Section 4: Access Control

Overview

This section provides an overview of the various policies and standards surrounding access to confidential data such as SSN, and how to provide proper management and restrictions necessary for the protection of this data at the University of Washington.

Access Management

Access management is a set of processes that manage the entire lifecycle of access rights and privileges. It ensures that only authorized users are able to use resources and data, while preventing access to those who should not have access. Access management processes and best practices are part of routine operations and risk management. In aggregate, they help the UW implement and comply with related information security policies.

Policy Basics

A fundamental policy objective of the UW information security framework is to prevent disclosure of sensitive information to unauthorized people. Several UW administrative policy statements, standards, and guidelines reinforce this objective. The following citations provide a quick summary of these policies in relation to access management principles, outcomes, and expected operating practices.

- Grant access to all users based on the principle of least privilege where required. (APS 2.1, Section 6.e)
- Grant access to all users based on the principle of separation of duties where required. (APS 2.1, Section 6.e)
- Support regular review and control procedures that ensure that all access privileges are current and appropriate. (APS 2.1, Section 6.f)
- System access accounts for users must be based on a unique identifier, and no shared account is allowed except as authorized by the system owner or operator and where appropriate accountability can be maintained. (APS 2.1, Section 7.d)
- Documented procedures should be in place for issuing, altering, and revoking access privileges on shared systems. (APS 2.1, Section 7.d)
- The approach taken at the UW is to adopt a classification scheme for all data and to define measures and practices that provide appropriate protection for each class of data. (APS 2.10, Section 1.a)
- Confidential data requires access control measures (authorization) that is documented and audited for compliance once every three years. (APS 2.10, Section 4.d)
- Confidential data requires data sharing agreements (with business partners, vendors and others who are given UW data.) (APS 2.10, Section 4.d)
- Management processes adopted to support the access control mechanisms should be sensible, reasonably easy to maintain, and auditable. For shared systems, they should include an electronic or paper request and approval process for all accesses established, modified, or terminated. The system owner/operator and data custodian should maintain this process. In addition, management processes

should include a regular process to review existing access accounts to ensure they are still valid. (UW Guidelines for Implementing Systems and Data Security Practices, Access Control Measures Section)

- A key security measure that system owners/operators need to implement is a means to authenticate system users. There must be a systematic and reliable method for establishing proof of identity. (UW Guidelines for Implementing Systems and Data Security Practices, Authentication Mechanisms Section)

Questions to Consider

1. How will the data be accessed? Describe how transactions and log-in validation are logged and audited in systems using SSNs.

2. How many individuals will have access to SSNs? Describe their role for each stage of the process.

3. Do you have procedures for adding or removing access privileges to SSN data for individuals who arrive, depart, or change roles?

Best Practices

This section outlines a series of best practices related to access management. When combined they can help ensure the availability, confidentiality, and integrity of confidential data over time.

1. **Clarify access management roles and responsibilities.** Data custodians, system owner/operators, business sponsors, service managers, and service desk managers should work together to clarify shared expectations related to access management. Educate each other on what each access privilege does from both a technical perspective and a business perspective. Decide who's accountable for compliance and risk management decisions, and who's responsible for reviewing and reporting access at an operational level. Teamwork and communication will ensure smooth, efficient operations.

2. **Schedule and plan for access reviews.** Determine how often access must be reviewed. Reviews are often conducted on a periodic schedule (e.g. monthly, quarterly) or driven by specific events (e.g. when an employee separates from the UW or changes departments). Decide how supporting data about privileges will be collected and to whom this data will be distributed for review. Decide how remediation decisions on inappropriate privileges will be reported and acted upon to remove access, including validating and documenting that necessary updates and removals have occurred.

3. **Support the job of reviewing access.** The job of reviewing and attesting that current assigned privileges are appropriate is made easier with supporting tools and documentation. It is critical that reviewers understand the criterion by which a given privilege is valid - just because someone has access doesn't mean they need access or should have access! If a reviewer isn't sure, they should be supported by clear and available documentation of the applicable access control policy: it should tell them who should and who should not have access, and who can authorize the privilege of access.

4. **Document procedures for requesting and approving access.** Users who request access should be aware of the criteria used to approve access, including demonstration of business need and any terms of use they may need to agree to prior to receiving access. When documenting approval procedures, include the evaluation criteria that supports decisions on who is entitled to access. This will make it easier to determine what privileges to assign and how they map to technical role/groups.

5. **Document technical access control/configuration procedures.** System owner/operators can support the access management process in several ways. System security models, data flow diagrams, and technical access control measures should be documented to facilitate the overall objectives of access management. Operationally, when access has been approved or revoked, documented procedures and checklists for configuring access and handling exceptions can help ensure changes are applied quickly and correctly. A

catalog of standard technical roles/groups used to control access to assigned privileges is also recommended where applicable and should be managed and reviewed, like the privileges themselves, to remove obsolete roles/groups and corresponding access.

6. **Monitor for significant status changes.** Successful access management processes are sensitive to events that trigger review or automatic removal of privileges. For example, where access is provided to users based on UW employment status the following might imply immediate need to reassess the validity of current assigned access privileges:
    a. Job changes/promotions/demotions
    b. Job transfers (e.g. between units)
    c. Unit reorganization that changes staff roles/responsibilities
    d. Resignation, retirement, separation, or death
    e. Disciplinary action or dismissals
    f. On leave status

7. **Monitor access logs for inappropriate use.** Be prepared to make use of log files to ensure proper use, detect intrusions and abuse of access privileges, and support forensic investigations. Access management processes often rely on the ability of system owners/operators to report incidents appropriately and provide timely evidence of access (e.g. dates, times, actions).

8. **Document procedures for removing access privileges.** Just as access requests and approvals benefit from procedural support, document how privileges will be removed. Consider scenarios where removal is being requested and the evaluation criteria by which decisions are made. Who has authority to remove access on behalf of another (e.g. business team, employee's supervisor)? What are the steps by which access is removed, validated, and communicated as needed?

9. **Never share passwords.** Passwords protect logins. Always log out when leaving a computer station. Do not share your password or login to systems using your access for others

10. **Secure your passwords.** Avoid writing passwords down or storing them in your desk. Never use the "remember my password" feature. Change passwords frequently and avoid using easily identifiable information for a password. Use a combination of letters, numbers, and symbols.

11. **Consider physical security.** Paper files, backup tapes, disks, and other portable media with confidential data should be kept in locked cabinets and keys should be strictly controlled.

Resources

There are local and external tools and resources to help you implement and maintain appropriate access management processes. Here are some examples:

- **UW Human Resources.** Provides an **on-boarding toolkit** and **separating employee checklist** for supervisors.

- **UW Information Technology.** Offers **Identity and Access management** tools and resources for access management (including ASTRA).

- **UW Internal Audit**. Offers services focused on financial, operational, and compliance related controls to support ongoing operations.

- **Office of Risk Management.** Helps University faculty, staff and students identify and reduce risks associated with their activities.

- **PASS Council.** Provides key support services for University-wide compliance requirements.

- **Office of the Chief Information Security Officer.** Offers support to protect confidential data through policies, standards, and continued education / awareness.

- See also ITIL v3.0 (which includes Access Management as part of Service Operation), ISO/IEC 27002, and other industry best practices.

Section 5: Data Protection

Overview

This section provides an overview of the various ways data can be protected from misuse at the University of Washington. This section assumes the following steps have already been taken, and that SSN data has been identified which needs to be protected:

- Identified applications that use data
- Identified servers (where data is stored)
- Identified data flows (how data moves)
- Verified that you actually need SSN data. Purge if not necessary. (See Section 6)

Questions to Consider

1. How will the sensitive data be secured? (Both electronic and non-electronic forms)

2. Does your department store confidential data such as SSN on laptops, USB drives, smartphones or other portable devices?

3. Are your department's computers which contain confidential data in compliance with the UW Minimum Data Security Standard (APS 2.10)?

4. What is your department's protocol for testing upgrades for the systems and software using SSNs?

5. If you are a Nebula client, have you discussed your data security requirements with your Nebula support person?

Best Practices

1. The best way to protect SSN data is to have as few copies of the data as necessary (with zero copies being the ideal number).

2. Confidential data is easier to protect if it is kept on well-managed servers in secure data centers and accessed only from well-managed desktop systems; the need to keep SSN data in other places (laptops, home systems, smartphones, etc) increases the risk and cost of management.

3. If at all possible, never use real SSN data for development, test, and evaluation systems - unless those systems are being managed to the same standards as the production system.

4. You must follow the Minimum Data Security Standards as defined in UW Administrative Policy Statement 2.10. If you are unable to follow the standards you must receive an exception from the PASS Council and the executive management of your department. Refer to APS 2.10 for more details:

    - Only use or reside on a controlled computer (configuration control + change management) that meets minimum computer security standards
    - System logs reviewed and alerts configured
    - Two-layer authentication (minimum)
    - Firewall protections

- Physical security
- Encryption during transmission
- Encryption during storage/backup - recommended
- Encryption at rest (on file system or in database) - recommended
- Data Sharing agreements - required

Technical Tools

The following technologies can be used to address each of the requirements above to protect confidential data such as SSN. Due to the variety of technologies in use at the UW, this list is neither complete nor authoritative. This list is intended to be a guide to help you discuss and find solutions to meet your data protection requirements with your System Operators, System Owners, Data Stewards, and the Office of the Chief Information Security Officer (CISO). Note that units within the UW may have stricter policies and guidelines than these minimums.

Run systems containing confidential information as a "Controlled Computer"

- The term "**controlled computer**" is defined in the UW Administrative Policy Statement 2.10, Minimum Data Security Standards.
- UW provides site licensed AntiVirus software (**Sophos**).
- Verify who has access to the system and how the access is managed.
- For servers which are managed by a vendor or third party, verify their operational and security practices for the system (network access, enabled accounts, encryption, default passwords, etc.).

System logging - both Windows and Unix operating systems have logging mechanisms built in. Applications may also provide custom logs that should be reviewed regularly and watched for anomalies.

- Unix syslog, Windows event log
- Firewall logs (windows firewall, IPtables, hostallow/hostdeny)
- Splunk and 'system event correlator - SEC' are unix tools to help watch logs
- Microsoft System Center Operations Manager also monitors for system events and audit log monitoring

Two-layer authentication (usually the 'something you have' such as an electronic token)

- SecurID / Entrust tokens can be used on UW Technology managed servers, and web sites with Pubcookie authentication
- Digital Certificates on USB tokens are used by some systems for user authentication

Firewall security can be implemented at the application, host, or network layer. Examples include:

- Unix IPtables, Windows Firewall. Recommend closing all ports. Open specific ones as needed.
- Review all network applications running on computers. Turn off all but essential ones (netstat).
- Restrict access to ports as much as is manageable. Common examples are to restrict connections to specific IP addresses, subnets, or UW campus. Note that our wireless networks do not require authentication to use, so you may want to exclude or require additional authentication from those subnets.

Physical security of computers and backup tapes

- Review the physical access control for systems (door locks, keys, video cameras, badge readers)
- Video cameras may have certain restrictions on where they may be placed. Check with your management before installing a video monitoring system.

Encryption during transmission over the network (where the network can be any of: LAN, WAN, wireless, or cellular) can utilize the following protocols:

VPN, IPSEC
RDP (remote desktop), VNC, Citrix Viewer
HTTPS
SSH, SFTP, SCP
Kerberos
CIFS/NFS when used with Kerberos encryption

Email - email is generally difficult to encrypt both in transit and in personal file storage, so it should not be used to transmit confidential data (except if using encrypted attachment files). If you receive email with SSN data included in it, you should verify the data is removed from the email system as quickly as possible. If vendors or customers need to exchange confidential data with you, consider more strongly encrypted alternatives such as SFTP or SCP.

Encryption during storage/backup - Backup data is required to be encrypted when it contains confidential data (on site and off site), since tapes can be lost or stolen. If you use a third party backup service provider, verify the data is encrypted before you provide it to them, or that they encrypt the data before it is transferred to them, and when it's at rest on the backup tape or other storage medium.

Encryption at rest

- **Portable media (USB, smart phones, CD/DVD, cd, etc).** Storing data on portable media is high risk and should only be done when absolutely necessary. USB devices should have strong built-in encryption (IronKey), and cell phones should provide encrypted storage for local data, and be managed such that they have a 'remote erase' function in case they are lost or stolen.
- **Laptop computers** - every laptop that has SSN data should have its entire hard disk encrypted. Microsoft provides 'BitLocker' software to do this, and other third party products such as TrueCrypt exist for both Windows and other operating systems.
- **Servers** - It is recommended their data at rest be encrypted, but not required (risk of exposure is much less). The same technologies used by laptops can be used on servers.
- **Data Encryption at the application layer is also a possibility**. Some databases can store data in an encrypted format, or store only parts of the entire data (last 4 digits of SSN for example).

Document Imaging systems - note that the State needs to approve an imaging system if you plan to destroy original documents. For approval or recommendations on the approved imaging systems, please contact UW Records Management.

Data sharing agreements – are required if you are sharing confidential information including SSN with a vendor or other external entity. These provide an audit trial and help document each party's responsibilities and liabilities related to the confidential data.

http://www.washington.edu/admin/purchstores/docs/security.pdf

Section 6: Data Removal

Overview

The last step in appropriately handling confidential data including SSN is to securely remove it as soon as it is not needed. Reasons include:

- The data has reached the end of its official retention period
- You have changed your business processes and no longer need SSN
- You are replacing computers or other equipment whose storage contains SSN

UW Records Management Services manages and oversees compliance with state and federal laws and regulations related to the preservation and destruction of electronic media and paper information. Data retention schedules are determined by the function and type of record. Once data has reached the end of the specified retention period and is considered obsolete, it should be purged or destroyed.

If you have a system which uses SSN as an identifier and you would like to replace SSN with another identifier, (e.g. EID), please contact the appropriate Data Custodian for assistance. (UW HR for employee SSN; Registrar for student SSN.)

Questions to Consider

1. If you no longer need SSN, how will you securely dispose of all electronic and non-electronic records containing SSN?

2. Can you locate backup tapes or other storage containing SSN?

3. Do you have copiers or FAX machines that process documents containing confidential information such as SSN?

4. Do you print documents containing confidential information such as SSN?

Best Practices

1. Shred paper and electronic media (CDs, DVDs) containing confidential data such as SSN.

2. Use secure data deletion tools to wipe confidential data; don't rely on dragging files containing confidential data to the Recycle Bin or Trash Can.

3. Computers which contain confidential data should have their hard drives destroyed before being surplused. Contact UW Surplus Properties for disposal assistance.

4. Retain an audit log of purged, deleted, or destroyed confidential data. See the 'Tracking Sheet for identified SSN Usage' in Appendix 1.

5. When removing SSN from data bases, remember to destroy backup copies.

6. Many printers, copiers, and FAX machines retain copies of information in their internal memory. If you print, copy, or FAX confidential data, handle those machines with the same precautions as computers containing confidential data.

Resources

1. UW Records Management Services:
    a. Website (**http://www.washington.edu/admin/recmgt**)
    b. By phone 206-543-0573
    c. By email **urc@uw.edu**

2. Secure data deletion tools to assist you with a complete 'wipe' of your data:
    a. BCWipe from Jetico Inc. (jetico.com)
    b. CyberCide from CyberSrub LLC (cyberscrub.com)

3. Shredding services (paper and electronic media)
    a. American Data Guard, 206-285-5955
    b. Iron Mountain, 800-899-4766

4. Surplus computers that contain protected data
    a. UW Facilities Services, Moving & Surplus, surplus@u or 206-685-1573
    b. Assistance with wiping drives and surplus preparation, UW IT Computer Maintenance Group, cmg@u or 206-543-7865

Appendix 1: Worksheets

SSN: Data Inventory Worksheet

Process/Form/System: _____

Date: _____

Do you use any paper forms or electronic systems or any other means to?

YES/NO	(Please extend lists as necessary.)	Quantity (# of records)	Electronic/paper/other
	Solicit or collect SSNs? *(Please indicate the approximate number (#) of records contained in the file)* **Examples:** paper or electronic forms; over the counter or phone ID validation 1. 2. 3.		
	Store SSNs? **Examples:** paper files in cabinets; electronic database; backup tapes, etc. 1. 2. 3.		
	Use SSN as an identifier? **Examples:** account number; key field in a database; look-up field in a database 1. 2. 3.		

YES/NO	(Please extend lists as necessary.)	Quantity (# of records)	Electronic/paper/other
	Use SSNs in interactions with other systems at the University? **Examples:** send a feeds; send/share a departmental 1. 2. 3.		
	Share SSNs with third parties outside the University? **Examples:** receive standardized test scores; send compliance documents to the state or federal governments; process loans or vendor payments; share research data with collaborators or grantors 1. 2. 3.		
	Have archived or other "old" records that include SSNs? (i.e. employment records prior to the establishment of Employee Identification Numbers (EID) February 2002) **Examples:** file cabinets with old grade reports and class rolls; research data (including subject payment information); employee work profiles; data CD or DVDs; back-up drives and tapes 1. 2. 3.		
	Display SSNs on any documents or screens?		

YES/NO	(Please extend lists as necessary.)	Quantity (# of records)	Electronic/paper/other
	Examples: electronic reports; printed reports; spreadsheets; database views; forms 1. 2. 3.		
	Include SSNs on any mailed documents? **Examples:** letters to students, employees or patients regarding their status, accounts, benefits, etc.; transcripts 1. 2. 3.		
	Transmit SSNs over the Internet or through other data Connections (incl. fax)? **Examples:** exchange data sets via FTP/HTTP/P2P; host online databases; fax completed forms or reports to other units or entities 1. 2. 3.		
	Send SSNs in e-mail? **Examples:** exchange information with University colleagues when helping a employees and/or students; request ID validation; request information to assist with look-up; send/receive reports and files 1. 2. 3.		

YES/NO	(Please extend lists as necessary.)	Quantity (# of records)	Electronic/paper/other
	Store items with SSNs in a document imaging system? **Examples:** Image system; electronic back-ups of paper files 1. 2. 3.		

SSN: Documents - Tracking Sheet

Computer Name/Designation	Computer Location	Primary User	Date Reviewed	Reviewed By	Sensitive Data Found (Y/N)	Date Sensitive Data Removed	Removed By
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							
11.							
12.							
13.							
14.							
15.							
16.							

Tracking Sheet for Identified SSN Usage

Enter each process or system utilizing SSNs identified on your SSN Data Inventory Worksheets in the table below. Indicate those items for which SSN can be eliminated and those for which you plan to continue SSN. Indicate all your remediation plans for eliminated uses on the **SSN Remediation Plan** (below).

Process/System	Owner/Contact	Eliminate Use	Continue Use
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			

SSN: Remediation Plan

For each SSN usage identified for elimination on the **Tracking Sheet for Identified SSN Usage**, please describe your remediation plan below. Extend the form as needed.

SSN Usage to be Eliminated	Remediation Plan
[EXAMPLE – may be deleted from final report] *Employment Tracking involving paper form and departmental database*	*a. Replacement: The database will be converted to use University ID number rather than SSN as the key. The form will be updated to ask for University ID number.* *B. By when: the change will be made during summer 2010 to be ready for the fall 2010 use.* *c. How historical data will be handled (backups, archives, paper files): Paper copies of the forms are disposed of annually; the last batch with SSNs will be securely shredded in June 2010. The database backups are done on daily, weekly and monthly cycles; the backups containing SSN data should cycle out 6 months after the conversion, and the tapes will be securely destroyed.*
[EXAMPLE – may be deleted from final report] *SSN storage on individual machines (i.e. old grade sheets, old administrative reports)*	*a. Replacement: SSNs will not be stored on local machines other than those explicitly approved (see attached form).* *B. By when: We have reviewed/scanned all machines in our*

	department and begun removing non-approved data. All such data will be removed by XX/XX/XX; machines used regularly by those handling personal data will be re-scanned periodically (frequency based on risk). *c. How historical data will be handled (backups, archives, paper files): This data will cycle out of backups within 6 months of XX/XX/XX as described above.*
1.	a. Replacement b. By when c. *How historical data will be handled* (backups, archives, paper files)
2.	a. Replacement b. By when c. *How historical data will be handled* (backups, archives, paper files)
3.	a. Replacement

	b. By when c. *How historical data will be handled* (backups, archives, paper files)
4.	a. Replacement b. By when c. *How historical data will be handled* (backups, archives, paper files)
5.	a. Replacement b. By when c. *How historical data will be handled* (backups, archives, paper files)
6.	a. Replacement

	b. By when c. *How historical data will be handled* (backups, archives, paper files)
7.	a. Replacement b. By when c. *How historical data will be handled* (backups, archives, paper files)
8.	a. Replacement b. By when c. *How historical data will be handled* (backups, archives, paper files)

Prepared by: Administrative Contact

Name: _____ Title: _____

Signature: _____ Date: _____

Prepared by: Technical Contact

Name: _____ Title: _____

Signature: _____ Date: _____

Appendix 2: SSN Questionnaire

Understanding your data

1. What are the business needs and/or legal requirements for using SSNs?

2. Is there an alternative identifier that would suffice, such as Employee ID Number (EID), UW NetID, Student Number, or other? If so, see Section 6, Data Removal, for information on how to securely remove SSN from your files.

3. What other personally identifying data elements will be used in conjunction with SSN as part of the process (e.g. name, date of birth, address, phone number, etc.)?

4. How will you inform individuals (a) whether they are legally required, or may refuse, to supply their SSN, and (b) of any consequences of providing or not providing their SSN?

Where does it reside

1. How does the information flow? Include all points where SSNs are:
    a. Solicited or collected (e.g. paper forms, web forms, or data feeds from other systems)
    b. Loaded into a system
    c. Used in interactions with other UW systems
    d. Shared with third parties outside the UW
    e. Displayed on documents, printed reports, or screens
    f. Included on mailed documents
    g. Transmitted over the Internet or other data connection, including FAX
    h. Sent via e-mail
    i. Stored in a document imaging system
    j. Backed up or archived
    k. Completing the Inventory Worksheets and Data Flow Diagrams are an effective way to document this.

2. If the SSN will be shared with another organization (inside or outside the UW), how will it move between entities (both electronically and non-electronically)?

Access control

1. How will the data be accessed? Describe how transactions and log-in validation are logged and audited in systems using SSNs.

2. How many individuals will have access to SSNs? Describe their role for each stage of the process.

3. Do you have procedures for adding or removing access privileges to SSN data for individuals who arrive, depart, or change roles?

Data protection

1. How will the sensitive data be secured? (Both electronic and non-electronic forms.)

2. Does your department store confidential data such as SSN on laptops, USB drives, smartphones or other portable devices?

3. Are your department's computers which contain confidential data in compliance with the UW Minimum Data Security Standard (APS 2.10)?

4. What is your department's protocol for testing upgrades for the systems and software using SSNs?

5. If your department uses Nebula, have you discussed your data security requirements with your Nebula support person?

Data removal

1. If you no longer need SSN, how will you securely dispose all electronic and non-electronic records containing SSN?

2. Can you locate backup tapes or other storage containing SSN?

3. Do you have Copiers or FAX machines that process documents containing confidential information such as SSN?

4. Do you print documents containing confidential information such as SSN?

Appendix 3: Best Practices

Understanding your data

1. Use the SSN Standard and UW and departmental policies to determine if the collection, use, storage, or disclosure of SSN is appropriate.

2. Understand the Retention Schedule for the documents which contain SSN. If the UW is not required to retain the document, securely destroy documents containing SSN as soon as possible (including paper, post-it notes, spreadsheets, microfiche, computer files, etc.) Don't keep copies of official documents which are being retained by another department. (e.g. I-9 and W-4 forms should only be retained in the UW Payroll Office.)

3. If you have identified a business need for SSN, consider masking part of the number (e.g. only display the last four digits: XXX-XX-1234.)

4. Be aware of disclosing sensitive information over the phone. Verify the caller. Obtain permission before leaving personal information on voice mail or answering machines.

5. Avoid asking for SSN over the phone. Is there another way to verify the identity of the caller? (EID, Student Number, address, etc.)

6. Be aware of conversations involving personal information. Can the conversation be overheard?

7. Require written consent or Power of Attorney before sharing personal information such as SSN with a third party (including spouse, parent, and relatives).

8. Don't collect SSN if it is not required; remove SSN from paper forms unless required.

9. Whenever possible, avoid sending documents containing SSN through campus mail; deliver in person.

10. SSNs and other sensitive information should only be FAXed to known parties where access to the FAX machine is limited and protected:

    - Notify the recipient in advance that sensitive information is being transmitted.
    - Indicate on the FAX cover sheet that the materials are confidential.
    - Confirm that the materials have been received.

Where does it reside

1. Complete the Inventory Worksheets and Data Flow Diagrams to assist you in making proper decisions regarding the collection, use, and disclosure of SSNs.

2. Store paper containing SSNs in a secure location such as a locked file cabinet.

3. Limit distribution of documents with sensitive information. How is the information maintained? Is the information exchanged?

4. All departmental application systems should be registered with the UW Application Portfolio, a comprehensive catalog of UW administrative applications and their functions.

Access control

1. **Clarify access management roles and responsibilities.** Data custodians, system owner/operators, business sponsors, service managers, and service desk managers should work together to clarify shared expectations related to access management. Educate each other on what each access privilege does from both a technical perspective and a business perspective. Decide who's accountable for compliance and risk management decisions, and who's responsible for reviewing and reporting access at an operational level. Teamwork and communication will ensure smooth, efficient operations.

2. **Schedule and plan for access reviews.** Determine how often access must be reviewed. Reviews are often conducted on a periodic schedule (e.g. monthly, quarterly) or driven by specific events (e.g. when an employee separates from the UW or changes departments). Decide how supporting data about privileges will be collected and to whom this data will be distributed for review. Decide how remediation decisions on inappropriate privileges will be reported and acted upon to remove access, including validating and documenting that necessary updates and removals have occurred.

3. **Support the job of reviewing access.** The job of reviewing and attesting that current assigned privileges are appropriate is made easier with supporting tools and documentation. It is critical that reviewers understand the criterion by which a given privilege is valid - just because someone has access doesn't mean they need access or should have access! If a reviewer isn't sure, they should be supported by clear and available documentation of the applicable access control policy: it should tell them who should and who should not have access, and who can authorize the privilege of access.

4. **Document procedures for requesting and approving access.** Users who request access should be aware of the criteria used to approve access, including demonstration of business need and any terms of use they may need to agree to prior to receiving access. When documenting approval procedures, include the evaluation criteria that supports decisions on who is entitled to access. This will make it easier to determine what privileges to assign and how they map to technical role/groups.

5. **Document technical access control/configuration procedures.** System owner/operators can support the access management process in several ways. System security models, data flow diagrams, and technical access control measures should be documented to facilitate the overall objectives of access management. Operationally, when access has been approved or revoked, documented procedures and checklists for configuring access and handling exceptions can help ensure changes are applied quickly and correctly. A catalog of standard technical roles/groups used to control access to assigned privileges is also recommended where applicable and should be managed and reviewed, like the privileges themselves, to remove obsolete roles/groups and corresponding access.

6. **Monitor for significant status changes.** Successful access management processes are sensitive to events that trigger review or automatic removal of privileges. For example, where access is provided to users based on UW employment status the following might imply immediate need to reassess the validity of current assigned access privileges:

    - Job changes/promotions/demotions
    - Job transfers (e.g. between units)
    - Unit reorganization that changes staff roles/responsibilities
    - Resignation, retirement, separation, or death
    - Disciplinary action or dismissals
    - On leave status

7. **Monitor access logs for inappropriate use.** Be prepared to make use of log files to ensure proper use, detect intrusions and abuse of access privileges, and support forensic investigations. Access

management processes often rely on the ability of system owners/operators to report incidents appropriately and provide timely evidence of access (e.g. dates, times, actions).

8. **Document procedures for removing access privileges.** Just as access requests and approvals benefit from procedural support, document how privileges will be removed. Consider scenarios where removal is being requested and the evaluation criteria by which decisions are made. Who has authority to remove access on behalf of another (e.g. business team, employee's supervisor)? What are the steps by which access is removed, validated, and communicated as needed?

9. **Never share passwords.** Passwords protect logins. Always log out when leaving a computer station. Do not share your password or login to systems using your access for others

10. **Secure your passwords.** Avoid writing passwords down or storing them in your desk. Never use the "remember my password" feature. Change passwords frequently and avoid using easily identifiable information for a password. Use a combination of letters, numbers, and symbols.

11. **Consider physical security.** Paper files, backup tapes, disks, and other portable media with confidential data should be kept in locked cabinets and keys should be strictly controlled.

Data protection

1. The best way to protect SSN data is to have as few copies of the data as necessary (with zero copies being the ideal number).

2. Confidential data is easier to protect if it is kept on well-managed servers in secure data centers and accessed only from well-managed desktop systems. The need to keep SSN data in other places (laptops, home systems, smartphones, etc) increases the risk and cost of management.

3. If at all possible, never use real SSN data for development, test, and evaluation systems - unless those systems are being managed to the same standards as the production system.

4. You must follow the Minimum Data Security Standards as defined in UW Administrative Policy Statement 2.10. If you are unable to follow the standards you must receive an exception from the PASS Council and the executive management of your department. Refer to APS 2.10 for more details:
    - Only use or reside on a controlled computer (configuration control + change management) that meets minimum computer security standards
    - System logs reviewed and alerts configured
    - Two-layer authentication (minimum)
    - Firewall protections
    - Physical security
    - Encryption during transmission
    - Encryption during storage/backup - recommended
    - Encryption at rest (on filesystem or in database) - recommended
    - Data Sharing agreements - required

Data removal

1. Shred paper and electronic media (CDs, DVDs) containing confidential data such as SSN.

2. Use secure data deletion tools to wipe confidential data. Don't rely on dragging files containing confidential data to the Recycle Bin or Trash Can.

3. Computers which contain confidential data should have their hard drives destroyed before being surplused. Contact UW Surplus Properties for disposal assistance.

4. Retain an audit log of purged, deleted, or destroyed confidential data. See the 'Tracking Sheet for identified SSN Usage' in Appendix 1.

5. When removing SSN from data bases, remember to destroy backup copies.

6. Many printers, copiers, and FAX machines retain copies of information in their internal memory. If you print, copy, or FAX confidential data, handle those machines with the same precautions as computers containing confidential data.