Social Security Number (SSN) 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.