VI.K. SOCIAL SECURITY NUMBER POLICY

(Source: Offices of the Vice President for Information Systems and Computing and the Associate Vice President for Audit, Compliance and Privacy, Almanac, December 18, 2007; revised April 6, 2010 *(*https://almanac.upenn.edu/archive/volumes/v56/n28/policies.html*))*

Authority and Responsibility

The Privacy unit within the Office of Audit, Compliance and Privacy is responsible for identifying major privacy-related risks that the University faces and coordinating appropriate responses to mitigate those risks. Information Systems and Computing is responsible for the operation of Penn's data network and infrastructure (PennNet) as well as the establishment of information security policies, guidelines, and standards. These offices, therefore, have a responsibility to develop a policy in response to the significant privacy, security, and compliance risks concerning Social Security numbers (SSNs).

Executive Summary

This policy establishes expectations around the use of SSNs - sensitive data whose misuse poses privacy risks to individuals, and compliance and reputational risks to the University. It calls on staff, faculty, contractors, and agents of the above to inventory their online and offline SSNs and reduce the above risks by, in priority order:

1. eliminating this data altogether,
2. converting it to PennID,
3. truncating the data to capture and display only the last four digits,
4. when the complete SSN is clearly necessary, ensuring strict security controls to protect the full data.

Purpose

This policy establishes a formal institutional program around SSNs for the purposes of protecting the privacy of Penn constituents and reducing compliance and reputational risks to Penn. This policy establishes clearly defined steps and announces available resources to reduce the availability of this sensitive data.

Risk of Non-compliance

SSNs are often, in the wrong hands, used by identity thieves to commit fraud by opening and using new credit accounts in a victim's name as well as gaining access to other personal and confidential information. In the case of credit abuse, the result is often a credit report damaged with inaccurate information reflecting the activity of the thief rather than the victim. This credit report can take months or more to correct and in some cases, results in lost opportunities for the victim and at times out-of-pockets costs. In non-credit cases, the damage could be exposure or abuse of private personal data of many sorts, including medical records, financial information, and other sensitive data. In addition, Pennsylvania and other states' "security breach notification" laws impose compliance obligations to notify data subjects of computer security breaches that expose full SSNs among other data. Individuals who fail to comply with the policy are subject to sanctions up to and including termination, depending on the nature, scope and severity of the violation, in accordance with University policies.

Definitions

Desktop or Workstation

A computer primarily used to provide direct access (via a locally attached keyboard, mouse and monitor) to applications such as web browsers, email clients, office productivity and data analysis tools for use usually by one individual.

Firewall

A device or a tool that restricts and or logs network traffic. Firewalls can be implemented in software, hardware or a combination of both on the host or at the gateway.

Key recovery

A special feature of a key management scheme that allows data to be decrypted by an authorized party even if the original key is lost.

Personal Computing Device

Any computer intended primarily for individual use. This includes, but is not limited to, Desktops, Workstations, laptop computers, PDAs, phones and data storage devices such as iPods, USB drives, CDs, DVDs, back-up media, etc.

Personal Digital Assistant (PDA)

A hand-held electronic device or organizer that has the capability of accessing, storing and/or transmitting data.

Server

A computer used primarily to provide network-based services (e.g. web, file, or email), typically for use by multiple users.

Social Security Number (SSN)

A nine-digit account number issued by the United States government, relating to an individual's account with the Social Security Administration.

Scope

A. The individuals subject to this policy are all faculty, staff, contractors, and their respective agents in connection with Penn-oriented functions and activities involving SSNs. This policy requires that Local Security Liaisons assist these individuals in developing compliance plans, where appropriate, and develop programs to promote compliance.

B. The information subject to this policy includes SSNs collected and maintained as part of University operations. For example, the handling of one's own SSN, or SSNs of family members, separate and apart from University operations is not subject to this policy, though many of the measures contained in this policy are recommended as a matter of best practice for such situations.

Statement of policy

General: Best Efforts to Identify and Reduce Availability of SSNs

It is the responsibility of individuals subject to this policy to use best efforts to know and inventory where they are maintaining SSNs and to make best efforts to securely delete, convert, truncate, or secure such information.

1. **Inventory of SSNs** The inventory requirement is met by:
    1. Identifying hard copy documents, including reports from information systems that contain SSNs.
    2. Identifying electronic files on Personal Computing Devices and servers including files stored in applications and databases, large and small - that contain SSNs. See Best Practices below.
    3. Identifying vendors, contractors, or agents with whom you are working who work with SSNs of Penn constituents as part of a Penn-sponsored activity.
2. **Remediation - Eliminate, Convert, or Truncate** In cases where complete SSNs are not necessary, and neither Penn's Records Retention Schedules nor applicable law require the retention of such information, the SSNs identified must be addressed in one of the following ways, in *priority order*:
    1. Securely destroy the information.
        1. Paper records may be securely destroyed by utilizing shredding services. For assistance in obtaining shredding bins or related records destruction services, contact the Penn Records Center at 898-9432. Recycling of paper records containing SSNs is prohibited under this policy.
        2. Electronic information may be securely destroyed using secure individual file deletion or secure disk wipe utilities. For resources regarding securely deleting electronic information, see References, below.
    2. Convert information to Penn ID or other identifier. Penn's Office of Information Systems and Computing must be consulted to employ the SSN-to-Penn ID conversion utility; this assistance is available free of charge. Any remaining files with SSNs, once converted, must be securely destroyed.
    3. Truncate SSNs.
    Collect, maintain, and display only the last four digits of SSN. Truncated SSNs, while still carrying some risk, are generally less harmful to individuals from a privacy perspective as compared to complete SSNs.
3. **Remediation - Securing Complete SSNs** In some cases, the maintenance of a complete SSN is necessary to comply with legal requirements or other business or IT processes that have not yet converted from SSN usage. Complete SSNs may also be necessary for certain Institutional Review Board-approved research activities. In such cases, this sensitive data must adhere to the following strict security standards:
    1. **Servers** - SSNs may only be stored on secure Penn servers that meet the requirements of Penn's Computer Security Policy (see References, below), as amended.
    2. **Desktops and Laptops** - SSNs may only be stored on desktops and laptops if
        1. the desktop or laptop meets the requirements of Penn's Computer Security Policy;
        2. the desktop or laptop is protected by a firewall;
        3. the data on the desktop or laptop is protected at rest with encryption, using strong encryption with a key recovery component;
        4. laptops storing SSNs additionally make use of software that allows for location tracking and remote secure wipe to provide additional protections in the event of loss or theft, except on systems for which the use of tracking software would interfere with the technical functionality or integrity of encryption software.

    Users should be aware that if encryption or tracking software is installed, a risk is created that data stored on the machine's hard drive may be damaged through operation of that software.

    3. **Personal Data Assistants and similar computing devices, USB drives, iPods and similar storage devices** - These devices, because of their portability, are at great risk of being lost or stolen. As a result, storage of SSNs on such devices is strongly discouraged. If storage is clearly necessary, the data must be protected at rest with encryption, using strong encryption with a key recovery component. In addition, where effective technology is available for the device, such device must also be equipped with a remote wipe / delete function and a firewall. Users should be aware that if encryption software is installed, a risk is created that stored data may be damaged through operation of that software.
    4. **Remote Access**
        1. **Encryption Requirement** - Any SSNs accessed remotely must be encrypted in transmission and must not be stored locally unless they are encrypted in accordance with this policy. ISC Information Security shall publish technical interpretations of this requirement (see References, below).
        2. **Public Computers / Computers with Significant Security Risk** - Do not use public computers, and other computers whose security is unknown, to gain remote access to SSNs. Similarly, do not use computers whose security is known to be insufficient to protect SSNs.
    5. **Need to Know Access** - Access to SSNs must be restricted to individuals with a need to know for University functions to proceed.
    6. **Securing Paper** - Any paper containing SSNs must be held in a locked file cabinet. Any such paper must be securely destroyed as soon as practicable consistent with Penn's Records Retention Schedules and applicable law.
    7. **Electronic Records - Secure Destruction** - Any electronic record containing SSNs must be securely destroyed as soon as practicable consistent with Penn's Records Retention Schedules and applicable law.
4. **Remediation - Use by Third Parties** SSNs will be released by the University to entities outside the University only when:
    1. permission is granted by the individual, or
    2. the external entity is acting as a University's contractor or agent and Penn has made reasonable efforts to ensure that the entity has adequate security measures in place to protect the data from unauthorized access, or
    3. as approved by the Office of Audit, Compliance and Privacy.
5. **Remediation - Restrictions on Transmission** - SSNs may not be sent over any network in plaintext (unencrypted), including e-mail. ISC Information Security shall publish technical interpretations of this requirement (see References, below). For one option, see number 5 in Best Practices, below.

Recommendations and Best Practices

1. **Inventory tools** - Automated tools are recommended as a best practice for locating files with SSNs. For information about what tools are available see Inventory Tools in References, below.

2. **Truncated SSNs as Authenticators** - Use of truncated SSNs as an authenticator is discouraged because it does not provide sufficient security. There may be limited situations where it is necessary to use truncated SSNs, in combination with other data, as an authenticator. Such situations should be remediated as soon as technically feasible.
3. **Reports from Central Systems** - Notify data stewards of central or other systems that continue to issue reports containing full SSNs.
4. **Consult with Security Liaisons** - Users of Personal Computing Devices storing SSNs should be encouraged to consult with Security Liaisons for the School or Center to assist in meeting the security requirements found in this policy.
5. **Secure Share** - For sharing documents that contain sensitive information, Secure Share is a safe alternative to file exchange methods such as e-mail, FTP, and portable devices.

Compliance

A. **Verification:** Through its annual program of risk-based audits and compliance assessments, the Office of Audit, Compliance and Privacy will verify that organizations are in compliance with this policy.
B. **Notification:** Violations of this policy will be reported by ISC Information Security and the Office of Audit, Compliance and Privacy to the Senior Management of the Business Unit affected.
C. **Remedy:** Violations will be recorded by the Office of Audit, Compliance and Privacy and any required action to mitigate harmful effects will be initiated in cooperation with the Senior Management of the Business Unit affected.
D. **Financial Implications:** The business units shall bear the costs associated with compliance with this policy.
E. **Responsibility:** Responsibility for compliance with the policy lies with all faculty, staff, contractors, and their respective agents in connection with Penn-oriented functions and activities involving SSNs. In addition, Security Liaisons must assist these individuals in developing a compliance plan, where appropriate, and develop other programs to promote compliance. Such programs may include: raising awareness, designating a day or week for SSN clean-up programs and annual reports of progress from divisions / departments within the School or Center. The Office of Audit, Compliance and Privacy, and Information Systems and Computing, are available for consultation in connection with developing compliance plans and achieving compliance.
F. **Time Frame:** Compliance with this policy shall be achieved no later than December 15, 2010; with the following exception: schools and centers following compliance plans established on or before May 1, 2008 shall not be deemed out of compliance with this policy on the ground of lateness, as long as they are adhering to their respective plan timeframes.
G. **Enforcement:** Individuals not adhering to the policy may be subject to sanctions as appropriate under Penn policies.
H. **Appeals:** Requests for waiver from the requirements of this policy may be submitted to either the Office of Audit, Compliance and Privacy or Information Systems and Computing, Information Security. These requests shall be decided by the Vice President of Information Systems and Computing and the Associate Vice President of Audit, Compliance and Privacy.

References

- **Shredding** - For assistance in obtaining shredding bins or related records destruction services, contact the Penn Records Center at 898-9432 http://www.archives.upenn.edu/
- **Computer Security Policy** - http://www.net.isc.upenn.edu/policy/approved/20100308-computersecurity.html
- **Inventory Tools** - One Step Ahead tip entitled "What's the Half Life of an SSN?," relating to Identity Finder software: https://almanac.upenn.edu/archive/volumes/v55/n25/osa.html
- **Requirement for Encryption of Data in Transit** - http://www.net.isc.upenn.edu/policy/supporting/20071120-ssnpol-tech-interpretation.html
- **Secure deletion of electronic files** - For resources regarding securely deleting electronic information, see http://www.upenn.edu/computing/security/privacy/data_clear.php
- **Secure Share** - https://www.isc.upenn.edu/security/secure-share (https://www.isc.upenn.edu/security/secure-share/)
- **SSN to PennID Conversion Tool** - Penn's Office of Information Systems and Computing must be consulted to employ the SSN-to-Penn ID conversion utility. Any remaining files with SSNs, once converted, must be securely destroyed. Contact 215-573-4492 to use the free SSN-PennID conversion tool.
- **Records Retention Schedules** - Penn's Records Retention Schedules may be found at http://www.archives.upenn.edu/urc/recrdret/entry.html