DRAFT POLICY **DRAFT POLICY** **DRAFT POLICY**

Policy draft in 30-day comment period, Sep 28, through Oct 27, 2007
Submit comments via email to 2007mmdd-ssnpol-comments@isc.upenn.edu

I. Title

A. **Name:** Social Security Number Policy

B. **Number:** 2007mmdd-ssnpol

C. **Author:** Lauren Steinfeld (Chief Privacy Officer and Institutional Compliance Officer) and Dave Millar (Information Security Officer)

D. **Status:**
[] proposed [X] under review [ ] approved [ ] rejected [ ] obsolete

E. **Date Proposed:** 2007-03-21

F. **Date Revised:**

G. **Date Approved:**

H. **Effective Date:**

I. **Compliance Date:** Compliance is to be achieved or, in the alternative, compliance plans are to be developed, no later than March 1, 2008.

II. Authority and Responsibility: The Office of Audit, Compliance and Privacy is responsible for identifying major 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.

III. Executive Summary: This policy establishes expectations around the use of Social Security numbers – 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 Social Security numbers 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.

IV. Purpose: This policy establishes a formal institutional program around Social Security numbers 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.

V. **Risk of Non-compliance:** Social Security numbers 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.

VI. Definition:

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.

VII. 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 Social Security numbers. This policy requires that Local Security Officers assist these individuals in developing compliance plans, where appropriate, and develop programs to promote compliance.
B. The information subject to this policy includes Social Security numbers collected and maintained as part of University operations. For example, the handling of one's own Social Security number, or Social Security numbers 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.

VIII. 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 Social Security numbers and to make best efforts to securely delete, convert, truncate, or secure such information.

A. Inventory of SSNs. The inventory requirement is met by:
   - i. Identifying hard copy documents, including reports from information systems that contain Social Security numbers.
   - ii. Identifying electronic files on Personal Computing Devices and servers including files stored in applications and databases, large and small – that contain Social Security numbers. See Best Practices below.
   - iii. Identifying vendors, contractors, or agents with whom you are working who work with Social Security numbers of Penn constituents as part of a Penn-sponsored activity.

B. 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 Social Security numbers identified must be addressed in one of the following ways, *in priority order*:

   - i. 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.
   - ii. Electronic information may be securely destroyed using secure individual file deletion or secure disk wipe utilities. For resources regarding securely deleting electronic information, see http://www.upenn.edu/computing/provider/recycle.html.
   - iii. 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.
   - iv. Truncate SSNs.

     Collect, maintain, and display only the last four digits of Social Security number. Truncated SSNs, as compared to complete SSNs, are generally less harmful to individuals from a privacy perspective.

C. 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:

i. Servers -- SSNs may only be stored on secure Penn servers that meet the requirements of Penn's Critical Host Policy (see: http://www.isc-net.upenn.edu/policy/approved/20000530-hostsecurity.html), as amended.

ii. Desktops and Laptops – SSNs may only be stored on desktops and laptops if
   1. the desktop or laptop meets the requirements of Penn's Critical Host 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,[1] using strong encryption with a key recovery component, within 3 months of such technology and service being recommended and supported at Penn;[2]
   4. if on a laptop, the laptop must contain software that permits, should the laptop be lost or stolen, location of the laptop and secure deletion of the data remotely ("tracking software").[3]

iii. 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 within 3 months of such technology and service being recommended and supported at Penn.[4] 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.

iv. 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
   2. Public Computers / Computers with Significant Security Risks – Do not use public computers, and other computers whose security is unknown, to gain remote access to Social Security numbers. Similarly, do not use computers whose

[1] 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.

[2] Schools and Centers considering an encryption solution independently should consult with ISC Information Security.

[3]See footnote 1 above.

[4] See footnotes 1and 2 above.

security is known to be insufficient to protect Social Security numbers.

v. Need to Know Access. Access to SSNs must be restricted to individuals with a need to know for University functions to proceed.

vi. 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.

vii. 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.

D. Remediation – Use by Third Parties

i. Social Security numbers 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.

E. Remediation – Restrictions on Transmission

i. SSNs may not be sent over any network in plaintext, including e-mail.

IX. Best Practices

A. Inventory tools -- Automated tools are recommended as a best practice for locating files with Social Security numbers. Information about what tools are available can be found at http://www.upenn.edu/computing/security/advisories/sensitive_data.html

B. Reports from Central Systems – Notify data stewards of central or other systems that continue to issue reports containing full SSNs.

C. Consult with Local Security Officers – Users of Personal Computing Devices storing SSNs should be encouraged to consult with Local Security Officers for the School or Center to assist in meeting the security requirements found in this policy.

X. Compliance

A. 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.
B. 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.
C. Financial Implications – The business units shall bear the costs associated with compliance with this policy.
D. 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 Social Security numbers. In addition, Local Security Officers 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.
E. Consultative Assistance – 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.
G. Time Frame – Compliance with this policy shall be achieved no later than March 1, 2008; in the alternative, a plan to achieve compliance with this policy within a reasonable timeframe shall be developed no later than March 1, 2008.
H. Enforcement -- Individuals not adhering to the policy may be subject to sanctions as appropriate under Penn policies.
I. 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.

XI. References

A. Shredding – For assistance in obtaining shredding bins or related records destruction services, contact the Penn Records Center at 898-9432.
B. Secure deletion of electronic files – For resources regarding securely deleting electronic information, see http://www.upenn.edu/computing/provider/recycle.html.
C. 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.

D. Records Retention Schedules – Penn's Records Retention Schedules may be found at http://www.archives.upenn.edu/urc/recrdret/entry.html.

DRAFT POLICY DRAFT POLICY DRAFT POLICY