SSN Protection Procedure

Contents

Introduction

The Social Security Number Protection Policy restricts the use of Social Security Numbers (SSN). The standards presented in this procedural document give specific guidance to assist in implementation of and adherence to the policy.

Principles and Standards

The collection, reporting, and storage of SSN in paper and electronic files will occur as required by law. The SSN will also be used for administrative purposes, where a unique identifier is needed to share and coordinate information between governmental or administrative agencies, or when the University ID has not been assigned and the SSN is the only unique identifier available.

Data stewards will have broad oversight of the processes and data under their jurisdiction Organizational units will provide the resources for converting existing systems from SSN-based to University ID-based. These areas should work closely together to determine the most cost effective means to improve the security of SSNs as well as the priorities for implementation.

Safeguarding the SSN is the responsibility of every employee and student at Iowa State University. Each dean, director, and department chair or their designees has the responsibility to address the standards set forth in this policy. These responsibilities include:

- assessing risks in their areas and reporting those risks to the head of the organizational unit
- identifying, planning, interfacing, and converting data as necessary for institutional use
- implementing procedures that limit the exposure and use of SSNs by staff
- training staff in these procedures

Where a SSN is currently used, it should be replaced with the University ID. Until this is accomplished, the first 5 digits of the SSN should be masked when displayed. The University ID will be used in all future electronic or paper systems, both purchased and in-house developed, as the primary identifier for students, employees, and other individuals doing business with the university. This standard is effective immediately.

A University ID may be created and assigned to each individual with a verifiable relationship to Iowa State University. There are multiple areas within Iowa State University that create and assign the University ID. If an SSN is required to initiate the relationship, the originating department will be responsible for safeguarding the SSN and providing the proper disclosure to the individual. Maintenance of the University ID is the responsibility of the ISUCard Office.

Whenever an individual is asked to disclose his or her SSN, a notice must be provided as required by Section 7 of the Federal Privacy Act of 1974 (5 U.S.C. § 552a), which requires the University to inform the individual whether the disclosure is mandatory or voluntary, by what statutory or other authority the number is solicited, and what uses will be made of it.

- The notice shall use text identical to text from an Appendix to this policy or such other text as may be approved by the Office of University Counsel.
- It is preferable that the notice be given in writing, but if at times it will be given orally, the providing organizational unit or employee shall implement procedures to assure and document that the notice is properly and consistently given.

Existing stocks of forms need not be reprinted with the disclosure notice; a notice may be appended to the form. Future forms and reprints of existing stock shall include a notice printed on the form and electronic forms may include a link to the appropriate notice. The disclosure statement is required only when asking an individual to disclose their SSN. It is not required for transactions that may contain an SSN already on file with the University.

Standards for Access, Transmission, Storage, and Disposal

Organizational units must develop and follow administrative, physical, and technical procedures to protect the confidentiality of records or record systems containing a SSN.

Access

Access to SSN shall be limited to those who need to use SSN for the performance of their job responsibilities.

- Data stewards will grant and revoke access to SSN. Ongoing monitoring of access is expected.
- Steps must be taken to ensure visual and auditory privacy of SSN.
- Individuals having access to SSN must use password screensavers with timeout periods or desktop locking.

Transmission

Sending SSN over the Internet or by email is prohibited unless done in a secure environment. Appropriate measures must be taken to ensure the confidentiality of fax and paper transmissions containing SSN.

- All electronic transactions and transmissions containing SSN must use industry standard security protocols.
- When SSN is shared with a third party, a written agreement must be entered into to protect the confidentiality of the SSN. Suggested language for this agreement is included in the Appendix.
- SSN should not be included in email text or attachments unless done in an encrypted environment. Not all email servers encrypt the transmission of messages and email sent between servers is usually not encrypted.
- SSN should be removed from paper forms and faxes unless required by law or determined to be necessary by the appropriate data steward.

- When SSN is exchanged on paper, steps must be taken so the number is not revealed. The SSN must not appear in an envelope window.
- Fax transmissions over phone lines (fax to fax) are secure if appropriate safeguards exist when faxing SSN to make sure the recipient's fax number is correct and the recipient does not leave the fax in an unsecured area. Fax transmissions involving computer networks (fax to computer, computer to fax, computer to computer) are not secure and should not include SSN.

Storage

Organizational units must actively work to remove SSN from electronic files, databases, images, and paper documents. Historical files, databases, documents, and images containing SSN may be maintained provided access to them is limited and secure.

- SSN should not be stored on a local workstation, laptop, floppy disk, CD/DVD, personal digital assistant (PDA), USB flash drive, or any other portable storage device. If storing SSN on such a device is necessary, the information must be encrypted and the device must be physically secured.
- Computer applications requiring SSN must store the SSN on a secure network server. Encryption adds another layer of security.
- Servers, tapes, disks, back-ups, and other electronic storage devices containing SSN must reside in secure physical locations.
- Documents and forms containing SSN must be stored in secure drawers/ cabinets with appropriate security.
- Anyone working with paper that contains SSN must take steps to secure that information.

Disposal

As SSN is eliminated from the normal course of business, organizational units must follow these standards for secure disposal.

- Prior to disposal, steps must be taken to destroy portable electronic storage devices, floppy disks, and CD/DVDs containing SSN.
- Prior to recycling or disposal, desktop, laptop, and server disks containing SSN must be erased (scrubbed) using current industry standards.
- Paper documents containing SSN should be shredded locally or disposed of in accordance with ISU's Confidential Document Destruction Plan.

Resources

- Student Records
- IT Security Policy
- ISU Code of Computer Ethics and Acceptable Use
- ISU Health Information Privacy and Security Policy (HIPAA)
- Faculty Conduct Policy (Breach of Confidentiality)
- Confidential Data Destruction Plan

Appendix A: Sample Social Security Number Disclosure Statements

Disclosure for the employment application process

Disclosure of your Social Security Number (SSN) at the time that you apply for employment is voluntary. Federal and State law protects the privacy and security of your SSN and Iowa State University will not disclose your SSN without your consent for any other purposes except as allowed by law. Disclosure of your SSN will be required for purposes of conducting background checks or verification of degrees. If you are employed by Iowa State University, disclosure of your SSN is mandatory under Federal Law for payroll and tax reporting purposes.

Disclosure for the payroll signup process

Disclosure of your Social Security Number (SSN) is requested for the personnel records system at Iowa State University. Federal law requires the university to report income and SSN for all employees to whom compensation is paid. An employee's SSN is collected, stored, and reported for payroll, benefits, internal verification, and administrative purposes. Federal and State law protects the privacy and security of your SSN and Iowa State University will not disclose your SSN without your consent for any other purposes except as allowed by law. The university is working to minimize the use of SSNs within its business processes. For a full description of the ISU Social Security Number Policy, please go to the Social Security Number Protection Policy.

Disclosure for the student application process

Disclosure of your Social Security Number (SSN) is requested for the student records system of Iowa State University. Federal law requires that you provide your SSN if you are applying for financial aid. Although an SSN is not required for admission to Iowa State, your failure to provide an SSN may delay the processing of your application. Your SSN is maintained and used by Iowa State for financial aid, internal verification, and administrative purposes, and for reports to Federal and State agencies as required by law. Federal and State law protects the privacy and security of your SSN and Iowa State University will not disclose your SSN without your consent for any other purposes except as allowed by law.

General mandatory disclosure

Disclosure of your Social Security Number (SSN) is required of you in order for Iowa State University to [state intended use of SSN], as mandated by [Federal] [State] law. Federal and State law protects the privacy and security of your SSN and Iowa State University will not disclose your SSN without your consent for any other purposes except as allowed by law. The University is working to minimize the use of SSNs within its business processes. For a full description of the ISU Social Security Number Policy, please go to the Social Security Number Protection Policy.

General voluntary disclosure

Disclosure of your social security number (SSN) is requested from you in order for Iowa State University to [state intended use of SSN]. No statute or other authority requires that you disclose your SSN for that purpose. Failure to provide your SSN, however, may result in [state what may happen if the individual fails to provide SSN]. Federal and State law protects the privacy and security of your SSN and Iowa State University will not disclose your SSN without your consent for any other purposes except as allowed by law. The University is working to minimize the use of SSNs within its business processes. For a full description of the ISU Social Security Number Policy, please go to the Social Security Number Protection Policy.