SSN Data Protection Training

Required for those with access to SSNs in University systems

Under the Illinois Identity Protection Act, all employees who have access to Social Security numbers in the course of performing their duties must be trained to protect the confidentiality of those numbers. This document serves as the mechanism to deliver that training.

Identity Protection Act

5 ILCS 179, also known as the Illinois Identity Protection Act, entered into effect on June 1, 2010. In addition to requiring training, this Act specifically prohibits certain uses of Social Security numbers, creates collection and protection requirements, and requires the creation and publication of an agency policy. The requirements of this Act apply from the point of collection to the time of destruction for such information.

University Policy

1.13 Identity Protection is the University policy that governs Social Security numbers in accordance with the Identity Protection Act. It is also written to meet requirements under the Family Educational Rights and Privacy Act (FERPA) and the Privacy Act of 1974.

Training

The following information provides the required instruction for those with access to Social Security numbers at the University. Expand and review each section to complete this training.

Under the Act, no person, or state or local government agency, may do the following:

1. Publicly post or display an individual's Social Security Number
2. Print an individual's SSN on any card required for the individual to access products or services
3. Require an individual to transmit his or her SSN number over the internet, unless the connection is secure or the SSN is encrypted
4. Print an individual's SSN on any materials mailed to the individual (through USPS or electronic mail) unless:
    a. State or federal law requires the SSN to be on the mailed document
    b. The document is part of an application or enrollment process and the SSN is included to establish, amend or terminate an account, or to confirm the accuracy of that SSN
    c. The SSN is not visible without opening the envelope
5. Require an individual to use her SSN to access a website
6. Use the SSN for any purpose other than the purpose for which it was collected

Under the Act, SSNs may not be collected, used, or disclosed unless:

1. Required to do so by state or federal law, or the collection, use, or disclosure is otherwise necessary for the performance of the agency's duties and responsibilities
2. The need and purpose for the SSN is documented before the collection
3. The SSN number that is collected is actually relevant to the documented need and purpose

Under the Act, there are some exceptions to the rules established:

- SSNs may be disclosed to employees, agents, contractors or subcontractors of a governmental entity, or disclosed to another governmental entity in order for the performance of duties and responsibilities, and as long as the person receiving the disclosed information has given to the original government entity a copy of their policy that explains how the recipient will comply with the Identity Protection Act.
- SSNs may be disclosed pursuant to a court order, warrant or subpoena.
  Collection and disclosure of SSNs can take place in order to ensure the safety of state and local government employees.
- SSNs may be collected, used, and disclosed for internal verification or administrative purposes.
- SSNs may be collected, used, and disclosed in order to locate a missing person, a lost relative or a person who is due a benefit.

If the state agency collects Social Security Numbers and uses them on forms/documents that might be subject to public inspection and copying (e.g., FOIA requests), then the state agency must redact the Social Security Numbers before the public inspection and copying takes place.

Guidance

Under the University 9.8.1 Data Classification Procedure, Social Security numbers are classified as highly restricted. It is important to review and understand what is required when working with highly restricted data. For the purposes of this training, we have compiled some guidance specific to working with SSN data.

When collecting SSN data, ask yourself the following questions:

- Do you have an appropriate disclosure statement?
  - Such statements must 1) indicate whether the submission is mandatory or voluntary; 2) indicate the authority by which it is requested; and 3) how it will be used.
- Is the data being created in a secure location?
  - SSN data must only be accessible to those that are approved to access such data. The location that the data is created needs to reflect that restriction.
- Are you creating a copy of the data when only access is necessary?
  - SSN data exists on various forms that may have a need to be copied for normal business operations. Try to limit cases where the number itself is present and rely on access to the original source when possible.
- If the data was collected on paper, is it secured to only authorized people?
  - Paper documents require special consideration for physical security. Locked cabinets in restricted areas of facilities is a minimum.

When transferring SSN data, ask yourself the following questions:

- Are you using a secure method for transferring the data?
  - In accordance with University procedure, highly restricted data cannot be emailed in any circumstances.
  - University applications such as SendTo, ImageNow, iPeople, Campus Solutions, and Slate are approved for secure collection and transfer of SSN data. If you have a question, feel free to reach out to the InformationSecurityOffice@ilstu.edu.
- Are you authorized to transfer the data?
  - SSN data cannot be released without specific authorization and consent in many cases.
- Is the receiving party authorized to have the data and are also using secure methods to collect and use it?
  - SSN data requires careful consideration whenever it is being sent. Just because the receiver is authorized does not mean they are aware of the requirements to protecting the data.

If and when SSN data is no longer needed, disposal of such records must be handled in accordance with the 7.1.55 Record Retention University policy.

Questions

If you have any questions, contact us at InformationSecurityOffice@IllinoisState.edu.