IDENTITY PROTECTION POLICY

The Identity Protection Act (Act) requires each State government agency to draft, approve, and implement an Identity-Protection Policy to ensure the confidentiality and integrity of Social Security numbers (SSNs) agencies collect, maintain, and use. 5 ILCS 179/37. The Office of the Senate President adopts the following Identity-Protection Policy (Policy) pursuant to the Act, 5 ILCS 179/1 *et seq* and the Personal Information Protection Act, 815 ILCS 530. The Policy is intended to help safeguard SSNs from unauthorized access and dissemination.

Appendix A of this Policy is a Statement of Purpose, as referenced below.

I. Prohibited Activities

The Office of the Senate President shall not:

A. Publicly post, publicly display, or intentionally communicate or make available to the general public in any manner an SSN.
B. Print an individual's SSN on any card required for the individual to access products or services provided by the person or the entity.
C. Require an individual to transmit an SSN over the Internet, unless the connection is secure or the SSN is encrypted.
D. Print an individual's SSN on any materials that are mailed to the individual, through the U.S. postal Service, any private mail service, electronic mail, or any similar method of delivery, unless State or federal law requires the SSN to be on the document to be mailed.

SSNs may be included in applications and forms sent by mail, including, but not limited to, any material mailed in connection with the administration of the Unemployment Insurance Act, any material mailed in connection with any tax administered by the Department of Revenue, and documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the SSN. An SSN that is permissibly mailed shall not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope without the envelope having been opened.

II. Use and Collection of SSNs

A. The Office of the Senate President shall not collect, use, or disclose an SSN from an individual, unless:
    1. required to do so under State or federal law, rules, or regulations, or the collection, use, or disclosure of the SSN is otherwise necessary for internal verification or administrative purposes;
    2. the need and purpose for the SSN is documented in a Statement of Purpose before collection of the SSN; and
    3. the SSN collected is relevant to the documented need and purpose.
B. The Office of the Senate President shall not require an individual to use his or her SSN to access an Internet website.
C. When an individual is asked to provide the Office of the Senate President with an SSN, Senators and/or staff shall provide that individual with a Statement of Purpose describing the reasons the Office is collecting and using the SSN. The Office of the Senate President shall provide the Statement of Purpose to any individual upon request.

D. When collecting SSNs, the Office of the Senate President shall request each SSN in a manner that makes the SSN easily redacted if required to be released as part of a public records request.

E. The Office of the Senate President shall dispose of all SSNs in a secure manner once it is no longer needed.

III. Access to SSNs and Training

A. Only employees required to use or handle information or documents that contain SSNs shall have access to such information or documents.
B. Employees required to have access to SSNs in any form shall be trained to protect the confidentiality of SSNs. Training shall include:
    1. How to identify SSNs;
    2. How to protect the confidentiality of SSNs in different contexts and formats from the time of collection through the destruction of the information; and
    3. What to do in the event the confidentiality of an SSN has been compromised.

IV. Exceptions

The prohibitions set forth in section (II) do not apply in the following circumstances:

A. The disclosure of SSNs to agents, employees, contractors, or subcontractors of a governmental entity or disclosure by a governmental entity to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the governmental entity must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under this Act on a governmental entity to protect an individual's SSN will be achieved.
B. The disclosure of SSNs pursuant to a court order, warrant, or subpoena.
C. The collection, use, or disclosure of SSNs in order to ensure the safety of: State and local government employees; persons committed to correctional facilities, local jails, and other law-enforcement facilities or retention centers; wards of the State; and all persons working in or visiting a State or local government agency facility.
D. The collection, use, or disclosure of SSNs for internal verification or administrative purposes.
E. The disclosure of SSNs by a State agency to any entity for the collection of delinquent child support or of any State debt or to a governmental agency to assist with an investigation or the prevention of fraud.
F. The collection or use of SSNs to investigate or prevent fraud, to conduct background checks, to collect a debt, to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act, to undertake any permissible purpose that is enumerated under the federal Gramm Leach Bliley Act, or to locate a missing person, a lost relative, or a person who is due a benefit, such as a pension benefit or an unclaimed property benefit.

V. Duties in Case of Breach

A. "Breach" is as defined in the Personal Information Protection Act, 815 ILCS 530/5.
B. In case of a breach, the Office of the Senate President shall promptly notify the individuals whose SSNs may have been compromised. Notice may be delayed if a law enforcement agent determines that notification will interfere with a criminal investigation.
C. The notification may be written or electronic. Substitute notice is allowed consistent with the provisions of the Illinois Personal Information Protection Act, 815 ILCS 530/12.
D. The notification shall include but is not limited to:
    1. The toll-free numbers and addressed for consumer reporting agencies;
    2. The toll-free number, address, and website address for the Federal Trade Commission; and

3. A statement that the individual can obtain information from these sources about fraud alerts and security freezes.

E. Notification shall not include information concerning the number of individuals affected by the breach.

F. If the Office of the Senate President has had a breach of security, it must submit a report to the General Assembly within 5 days of the discovery or notification of the breach. Such notification shall include details pertinent to the breach, any actions taken to prevent future breaches of security, and corrective measures the Office has or will implement as a result of the breach. . After submitting such report, the Office of the Senate President must annually submit a report listing any additional breaches of security and corrective measures.