Tier 1 Control Standards (State-Wide)

Collection and Storage of Personal Information

Standard ID
IOT-CS-SEC-103

Published Date
3/1/2008

Effective Date
3/1/2008

Last Updated
5/17/2017

Next Review Date
5/17/2018

Policy
08.0 Data Security (PR.DS)
  08.1 PR.DS-1
    08.1.1 Data-At-Rest
  08.2 PR.DS-2
    08.2.1 Data-In-Transit

Purpose
It is the State of Indiana’s duty to protect the personal information of its citizens and other individuals doing business with the State from unauthorized access or disclosure, and possible misuse or abuse. This standard is designed to establish awareness and provide guidance on the proper handling of Social Security Number (SSN) and other personal information maintained by or on behalf of the State of Indiana.

Scope
IOT Supported Entities

Statement
Agencies are responsible for the development, documentation and implementation of applicable procedures to effectuate the following:

- The State does not permit the use of a SSN as the primary identifier for any person or entity in any system, except where the SSN is required or permitted by law, and permitted by State policy. Systems established prior to this policy being put into effect should migrate away from use of SSN as the primary identifier as soon as possible.
- Where permitted by law and State policy, the SSN may be stored as a confidential attribute associated with an individual or may be used as an optional key to identify individuals for whom a primary identifier is not known.
- Individuals shall not be required to provide their Social Security number, verbally or in writing, at any point of service, nor shall they be denied access to those services should they refuse to provide a SSN, except where the collection of SSN is required by law or otherwise permitted by State policy. Individuals may volunteer their Social Security number if they wish, as an alternate means for locating a record.
- Except where the SSN is required by law, the State ID (PeopleSoft) replaces use of the SSN and will be used in all future electronic and paper data systems and processes to identify, track, and service individuals associated with the State.
- All newly developed or acquired application software should not store SSN as a data element except where the collection of SSN is required by law or otherwise permitted by State policy.
- Servers housing databases or records containing SSNs should be protected through access restrictions and other protective measures that ensure it is viewed only by those authorized (protective measures can include firewalls, encryption, etc.).
- Records containing an SSN should be stored on network drives with limited access. Individual workstations, laptops and other personal computers (PDAs) should not be used to store records containing SSNs. If they are, additional protective measures are required.
- IOT instructs agencies to use only networked drives for the storage of data. If mobility is needed an encrypted flash drive or encrypted laptop hard drive is the safest alternative. All other removable or transportable media (e.g., cassettes, CDs, DVDs,
(etc.) shall not be used to store SSNs and other confidential data.

- Agencies shall provide appropriate guidance in regard to producing printed and faxed materials. Appropriate physical security measures must be identified and mandated by agencies where physical forms of the data are produced.
- Subject to applicable document retention policies or unless required by law, when no longer required, paper documents and electronic media containing SSNs will be destroyed or disposed of using methods designed to prevent subsequent use or recovery of information.
- SSNs will be released to entities outside the State only where permitted or required by law.
- The State will limit access to records containing SSN to those individuals requiring access as determined by job function. Individuals permitted access to SSN will be instructed on the appropriate handling and protection of this data by their management or designated representative.

Roles
All Personnel

Responsibilities
All personnel are responsible for understanding the requirements of this standard and performing their job in accordance with the requirements written within it.

Management Commitment
Management is responsible for ensuring their agency is meeting the requirements written within this standard.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT where necessary to appropriately secure data in accordance with this standard.

Compliance
Agencies own and are accountable for the protection of personal information. Discovery of an unauthorized release of personal information (as defined in IC 4-1-11-3) must promptly notify their management, IOT’s CISO, and follow Incident Management and Planning Standard and the agency’s incident response plan. These steps are designed to ensure the appropriate execution of duties stipulated by IC 4-1-10. Release of personal information determined to be a violation of law must be reported to appropriate law enforcement agency. Any violation of this policy may be cause for appropriate disciplinary action, including dismissal.

Exceptions
No exceptions.

Associated Links
http://iga.in.gov/legislative/laws/2015/ic/

Associated Documents
Personally identifiable information