Tier 1 Control Standards (State-Wide)

Personal Information Protection

Standard ID
IOT-CS-SEC-104

Published Date
6/1/2006

Effective Date
6/1/2006

Last Updated
5/19/2017

Next Review Date
5/19/2018

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
Personal information of citizens must be protected. This is a paramount requirement of agencies having systems storing personal information such as social security numbers and credit card numbers. Such information is at its greatest risk of compromise when removed from the protective measures implemented in government facilities and by government networks. Information on flash drives, CDs, DVDs, laptops, home PCs and other forms of media (from here forward referred to as “mobile”) are susceptible to loss and burglary potentially placing confidential citizen data into unauthorized hands. Some business functions require mobile personal information to effectively deliver State services. In such cases, the procedures below address the authorization process and protective measures required to take personal information out of State facilities or off of the State network.

Scope
IOT Supported Entities

Statement
Collection

- Personal information shall be collected as outlined in the Collection and Storage of Personal Information standard.

Storage Protection

- Personal information shall be stored on networked servers and adequately protected by “layers” of protection provided by hardware, software, policy and procedures.
- Personal information shall be stored in “enterprise” databases with robust security capabilities. Storage in “personal” databases, spreadsheets and word processing documents is permitted only with agency authorization and with the increased protective measures put in place to address the increased risk of compromise (see Mobile Media Protection section below).
- Tape backups of personal information must be appropriately protected in transit and in off-site storage.
- Personal information shall never be stored on servers directly exposed to the Internet.

“Mobile” Media Protection

Some business functions require personal information to be accessed in a “mobile” environment to effectively deliver State services. In such cases, the procedures below address the authorization process and protective measures required to take personal information out of State facilities or off of the State network. It is important that agencies and state workforce members understand personal information
is at its greatest risk of compromise when removed from the protective measures implemented in government facilities and by government networks.

- No confidential information shall leave State of Indiana facilities or networks on any media without authorization from the agency head or their designee. This includes information used by field staff for performance of job duties during normal working hours and all workforce members after hours.
- The authorization must detail specifically the personal information data elements, the media used to store the information, the duties to be executed, and duration. This information is to be maintained in a database.
- Personal information authorized for mobile media is protected through encryption technology approved by IOT. The encryption technology must protect either the full disk or all directories storing personal information.
- Personal information stored on mobile media (other than printouts) is copied regularly and stored securely on a state network. In case of theft or loss, this copy will be used to notify citizens of the loss.

**Mobile Media**

Mobile media includes but is not limited to:

- Laptops, notebooks, tablets
- Computers owned by the State storing personal information in homes or off-site
- PDAs, cell phones, Blackberry devices
- Flash drives, portable hard drives
- DVD, CD, diskette
- Printed reports

**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**

Violators of this policy are subject to discipline by their management up to and including dismissal.

**Exceptions**

No exceptions.

**Associated Links**

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