Tier 1 Control Standards (State-Wide)

System and Communications Protection

Standard ID
IOT-CS-SEC-147

Published Date
7/1/2015

Effective Date
7/1/2015

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
08.0 Data Security (PR.DS)
08.5 PR.DS-5

08.5.1 Asset Confidentiality

Purpose
This Standard summarizes the system and communications protection requirements for systems with confidential data.

Scope
IOT Supported Entities

Statement
The following controls are required for confidential systems:

- User functionality is separated from system administration responsibilities.
- The system functions so that the actions of a user are cleared after they complete the function. System resources are released back to the information system ensuring that no unauthorized and unintended information remains accessible by the next user of the system.
- Connections to external networks are explicitly authorized. External sites accessible are available only when approved by the system owner.
- Public access to systems with confidential data are designed/architected to mitigate the risks of unauthorized external access.
- Systems with confidential data shall have their servers isolated from other systems.
- Information transmissions are encrypted.
- Cryptographic mechanisms used by the system shall follow the Data Encryption Standard
- Mobile code (e.g. – JavaScript, Active X, etc.) is prohibited unless authorized by the system owner. A list of approved mobile code is maintained.
- The system has a name/address resolution service with built in redundancy
- Data at rest meets the requirements of the Data Encryption Standard.

Roles
Information Asset Owners/System Owners

Responsibilities
Information Asset Owners/System Owners must be aware of and meet the requirements related to system function and communication.
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 or communications in accordance with this standard

Compliance
Agencies shall attest to their compliance with these policies on an annual basis providing evidence as directed by the auditor or the CISO.

Exceptions
No exceptions.