Tier 1 Control Standards (State-Wide)

Media Storage

Standard ID
IOT-CS-SEC-142

Published Date
7/1/2015

Effective Date
7/1/2015

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
11.0 Protective Technology (PR,PT)
11.2 PR,PT-2
11.2.1 Removable Media

Purpose
This practice summarizes the media protection controls in place for State systems with confidential data.

Scope
All Devices that Connect to the State Network

Statement
The following controls are required for confidential systems:

- Media storage for the system shall be limited to server storage technologies (e.g. – SAN), backup media, and approved and audited outsourced services including Internet storage.
- System media storage shall be limited to the 2 data centers housing confidential systems components unless authorized by the agency.
- Confidential data shall be encrypted on all forms of media storage utilized.
- Any storage component at end-of-life or being replaced shall be sanitized digitally to compliance with DOD standards or physically destroyed.
- Printed reports shall be shredded after use.
- Printed reports to outside parties shall be sanitized of confidential information or ownership and the responsibilities that accompany it assigned to the new owner. These ownership responsibilities will be clearly defined and documented and agreed to by the new owner.
- System owner or their delegates shall confirm media sanitization upon removal and document the event.
- End user workstation hard drives shall be used for temporary files only. End users shall not store data from confidential systems on local drives, flash drives, CDs, DVDs, or on the Internet (e.g. - Dropbox, Box, Google) and other non-networked storage mediums without express authorization from the agency.

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 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