Removable Media

Standard ID
IOT-CS-SEC-012

Published Date
2/1/2017

Effective Date
3/1/2017

Last Updated
5/2/2017

Next Review Date
5/2/2018

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

Purpose
Limiting/restricting use of removable media helps prevent exfiltration of information from State systems, databases, and other data repositories.

Scope
All Devices that Connect to the State Network

Statement
Removable media (USB/Flash drives, Compact Disks, etc.) shall meet the following requirements:

- Read-only (i.e. data can be read and executed to a State machine) or block by default
  - Individuals/groups that require read/write privileges to perform essential job duties must have security coordinator approval, via helpdesk ticket. (i.e. data can be written to a USB)
  - Users with write privileges must be re-certified quarterly by security authorizers, that access is still required
- All removable media must be State provisioned, purchased through the State Quantity Purchase Agreement (QPA), or otherwise approved by the State CISO
- All personal, non-State issued removable media devices are not permitted for use
- All removable media that may contain Non-Public Information, must be encrypted using FIPS 140-2 compliant software, or otherwise meeting the requirements of the State’s Data Encryption Standard (IOT-CS-SEC-003)

Roles
All Personnel

Responsibilities
All parties must understand the removable media requirements and act in accordance with this Standard and the Information Resource Use Agreement (IRUA).

Management Commitment
Management shall review and quarterly evaluate users with removable media write-access to determine if it is still required for essential job duties.
Coordination Among Organizational Entities
Agencies shall coordinate with IOT when procuring removable media devices and when write access is needed.

Compliance
Individuals and/or agencies found to be out of compliance with this Standard will be escalated to the CISO and may be subject to disciplinary action.

Exceptions
Exceptions will be handled on a case-by-case basis by the State CISO.