Tier 1 Control Standards (State-Wide)

Operational Maintenance

Standard ID
IOT-CS-SEC-143

Published Date
7/1/2015

Effective Date
7/1/2015

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
10.0 Maintenance (PR.MA)
10.1 PR.MA-1
10.1.1 Asset Maintenance

Purpose
This practice summarizes the operational maintenance controls in place for the confidential systems system.

Scope
All Devices that Connect to the State Network

Statement
The following controls are required for confidential systems:

- Hardware and software maintenance shall only be provided by authorized support staff.
- Outsourcers shall define their operational maintenance procedures for agencies. If external maintenance providers are utilized, the procedures governing their use shall be known and audited.
- The system owner or their delegate shall understand and develop procedures to ensure appropriate oversight of all maintenance activities on their system.
- Maintenance records shall be kept by the system owner and shall include the date and time, the names of support staff performing maintenance, the system’s oversight delegate, a description of the maintenance performed, and a list of replaced components.
- Any component removed from the system shall be sanitized through compliance with DOD specifications or destruction.
- Maintenance tools shall be inspected for malicious code as part of the authorization process. Approved tools shall documented and the staff shall be trained on those tools available for use on their confidential systems.
- Support staff without access to the confidential systems system shall be given temporary IDs when necessary to perform needed duties. The IDs are to be disabled after maintenance is performed.

Roles
Information Asset Owners/System Owners

Responsibilities
Information Asset Owners/System Owners are responsible for understanding and maintaining confidential systems in accordance with this Standard.
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.