Tier 1 Control Standards (State-Wide)

Laptop Security

Standard ID
IOT-CS-SEC-128

Published Date
2/19/2008

Effective Date
3/1/2008

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
06.0 Access Control (PR.AC)
  06.3 PR.AC-3
  06.3.1 Remote Access

Purpose
To provide requirements for protection of laptops, notebooks, and or tablets and protect against potential loss of information stored on these devices. Within this practice, the term “remote devices” means any laptop, notebook, tablet, or other IOT supported equipment.

Scope
IOT Supported Entities

Statement
Physical Security

Agencies and users shall provide adequate physical security for all state-owned and state authorized remote devices. The following are requirements for mobile devices:

- Secure remote devices in a locked cabinet, a secure area of personal residence, or with cable locks when not in use.
- Don’t store passwords with the remote device.
- Don’t leave remote devices on car seats. Only leave the device locked in the trunk overnight when a safe spot in a facility or home is unavailable.
- Don’t store remote devices in checked luggage. Always carry it on.
- Track remote devices closely when going through airport screening.
- Record identifying information and mark equipment to enable its return in the event of a loss.

Operations and Maintenance

Agencies shall establish and implement IT security procedures, including training, for the secure operation and maintenance of remote devices. The following points should be covered procedurally:

- Remote devices must be password protected.
- Remote devices must have screen locking and screen savers in place.
- Remote Devices containing personal or sensitive information must have full disk encryption.

- Protect onlookers from viewing your screen and keystrokes in public locations (privacy filters may be required to ensure unwanted viewing of displayed information is prevented).
• Remote devices shall be equipped with IOT approved anti-virus and anti-spyware software and users will ensure that updates are loaded at appropriate intervals.
• Remote device operating systems shall be maintained with appropriate vendor security patches and updates.
• Mandatory system configurations, settings, and software for state-owned devices shall not be modified without prior authorization by IOT.
• Agencies shall perform regular data back-ups as frequently as needed based on the risk assessment of the information maintained on the device. Back-ups shall be safeguarded and retained for a period commensurate with the value and criticality of the information.
• Agencies shall develop guidelines on the management and maintenance of personal and state data on remote devices.
• Agencies shall develop policies and procedures for the return of state-owned devices when user employment is terminated.

Lost and Stolen Laptops

Remote devices will be stolen and lost. Agencies shall follow the guidance above to ensure that the worst event to happen is the loss of the asset rather than the compromise of information. Failures by agencies to adequately protect these devices shall be scrutinized and disciplinary measures handed down when appropriate. Further:

• Police reports must be filed with appropriate law enforcement agency.
• Lost or Stolen remote devices must be reported to the CISO.
• Incident management procedures should be followed within the agency (see Incident Planning and Management Standard).
• Additional media devices shall also be reported which could have contained state information. (USB drives, CDs, portable hard drives)

Education and Awareness

Agencies shall ensure that remote device security is addressed via awareness training prior to its provision and as new threats emerge that potentially impact the use of or risk to the asset.

Roles
All Personnel

Responsibilities

Personnel must understand the risks associated with remote devices and take steps to mitigate risks associated with the loss of the device or information stored on the device. IOT shall provide guidance on remote device security and support in the case of theft of the device or data.

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 on lost and stolen laptops, operational maintenance and education and awareness.

Compliance

Remote device security is the responsibility of the user assigned the device; however IOT will notify agency management of failure to comply with security guidelines if noted during routine equipment repairs, maintenance help desk calls etc.

Exceptions
No exceptions.