Tier 1 Control Standards (State-Wide)

Virus Control

Standard ID
IOT-CS-SEC-109

Published Date
2/1/2016

Effective Date
2/1/2016

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
08.0 Data Security (PR.DS)
08.6 PR.DS-6
08.6.1 Asset Integrity

Purpose
Agencies must protect the Information Resources from potential losses resulting from computer viruses and other malicious software. Within this practice, the term “virus” means any virus, worm, Trojan horse, or other malicious software. All devices connected to the state network shall be actively protected from viruses and other malicious software. All workforce members controlling devices that are connected to the state network are to ensure that their device is protected through functioning, current virus protection software.

Scope
All Devices that Connect to the State Network

Statement
All devices that connect to the State network must meet the following requirements:

- All state provided devices such as workstations, desktops, laptops, and servers connecting to the state network shall use the state standard, or IOT approved virus protection software installed. It shall remain activated with update capabilities enabled.
- Users may not change the configuration and/or remove IOT security software. Problems believed caused by virus protection software or software settings should be reported to the IOT Help Desk.
- All removable storage devices or media shall be scanned for viruses each time the device or media is connected to the state network.
- Non-state devices connecting from inside (in the case of contractors) or outside (personal devices) the state firewall must be authorized by the agency and shall have virus protection that meets or exceeds the state standard. Cost obligations for such software rest with the user if using a personal computing device.
- No workforce member may disable virus protection software unless approved by IOT during a troubleshooting exercise.
- All workforce members are responsible for immediately reporting to the IOT Help Desk any indication that a virus is present on a device they control that is, or may be, connected to the state network.
- Occasionally some software will not work with virus protection enabled. Those systems should be referred to IOT for review.

Roles
All Personnel

Responsibilities
All personnel should be aware of virus protection software and validate it is up to date.
Management Commitment
Management is responsible for ensuring their agency is aware of this Standard and takes appropriate steps to validate the

Coordination Among Organizational Entities
IOT support will configure anti-virus software initially and set a schedule to update software, it is the end user’s responsibility to ensure updates are properly running.

Compliance
The IOT Help Desk or desktop support may randomly check virus software settings as they conduct support duties.

Exceptions
Exceptions will be handled on a case by case basis through the Director of Risk & Compliance and State CISO.