Tier 1 Control Standards (State-Wide)

Virus Remediation

Standard ID  
IOT-CS-SEC-110

Published Date  
4/2/2009

Effective Date  
4/2/2009

Last Updated  
5/19/2017

Next Review Date  
5/19/2018

Policy  
13.0 Security Continuous Monitoring (DE.CM)  
13.4 DE.CM-4  
13.4.1 Malicious Code

Purpose  
Agencies must protect the Information Resources from potential losses resulting from computer viruses and other malicious software. When malware infections are identified, elimination of the malicious software and the resulting threats become an operational priority. All actions necessary shall be taken to protect against damage and further spread.

Scope  
All Devices that Connect to the State Network

Statement  
IOT technical support will take any and all actions necessary to eradicate malware from state computing devices upon discovery. Though IOT will combat the malware with as little user inconvenience as is possible, quickly addressing and eradicating the problem is the priority. The following ramifications may result from aggressive actions to eliminate malware threats:

- IOT shall implement proactive daily and weekly malware scanning processes that may adversely impact user performance.
- IOT shall inspect machines as necessary to identify details of the malware in order to protect other state devices from infection or to aid in troubleshooting.
- IOT shall take needed troubleshooting measures to minimize the damages to Information Resources. These actions may be taken without prior user or agency notification. Appropriate follow-up communications will be provided by IOT.
- IOT shall reimage PCs if necessary, possibly resulting in the loss of information stored on local drives.
- IOT shall block Internet access of infected devices until devices are properly cleaned and/or reimaged.
- IOT shall notify agency management of malware coming from repeat offenders with three or more virus events within a time frame of three month or in the case of gross negligence on the part of users.

Roles  
IOT Personnel

Responsibilities  
IOT shall acquire and deploy appropriate processes and tools to meet the requirements within this Standard.
Management Commitment
Management shall take necessary actions as dictated by IOT Security when malware is detected on a machine within their agency.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT Security on obtaining security metrics related to malware.

Compliance
Not applicable.

Exceptions
No exceptions.