

Statewide Information Security Standards

Standards Category: Information Security

Title: Statewide Antivirus and Anti-malware Standards

Number: S-107-03.1-10

Applicability: This policy applies to all Executive Branch agencies as defined in ORS 174.112, except as provided in ORS 182.122 and 182.124 and OAR 125-800-0020 (3)(a) and (b) and (4) as they apply to the State Board of Higher Education and the Oregon University System, the Oregon State Lottery, Secretary of State, State Treasurer, and the Attorney General.

Status: Adopted Draft Other: _____

Dates: (Effective Dates/Revisions/Reviews)

Effective: June 1, 2010 Revisions: N/A Scheduled Review by: June 1, 2012

Prepared by: DAS Enterprise Information Strategy and Policy Division (EISPD)

Adopted by: 
Dugan Petty, State Chief Information Officer

6/30/10
Date

Statutory Authority: ORS 182.122

Enterprise Standard:

Minimum -

3.1. Antivirus and Anti-malware Standards:

- 3.1.1 All workstations and Windows based servers shall have antivirus/anti-malware software installed upon them.
- 3.1.2 All information systems with antivirus software shall undergo at a minimum a monthly full system scan for viruses and malware.
- 3.1.3 Any information system with a virus, Trojan, etc. shall be removed from the network, and handled in accordance with incident response procedures.
- 3.1.4 Where technically possible, portable devices shall also have antivirus protection.
- 3.1.5 Where technically possible, antivirus/anti-malware software shall be centrally managed with ongoing updates and reporting.
- 3.1.6 Antivirus/anti-malware software shall be maintained at current patch level in accordance with the Patch Management Standards in section 4.6.
- 3.1.7 All antivirus/anti-malware signatures shall be updated and maintained at current vendor supported and recommended levels.
- 3.1.8 End users shall not be able to disable the antivirus/anti-malware software on their workstation or portable device.

- 3.1.9 All e-mail shall be scanned at the e-mail gateway and upon arrival at the workstation. Infected e-mail messages shall be isolated and remediated.

Recommended –

3.2 Antivirus & Anti-malware Recommended Best Practices:

- 3.2.1 Anti-malware solutions for workstations should be integrated with web browsing to scan for malicious web sites during browsing.
- 3.2.2 Monthly scans required in the Antivirus and Anti-malware Standards in section 3.1 should be scheduled to occur automatically.

Section (1) - Purpose and Objective: The goal of communications and operations management is to ensure the correct and secure operations of information processing facilities. This section describes security standards and best practices for Antivirus and Malware, Workstation Management and Desktop Security, Mobile Device Management, Server Management, Log Management, Information Backup, Security Zone and Network Security Management, Intrusion Detection and Prevention, Email, Remote Access, and Wireless Access.

Section (2) – Agency Deviations: In circumstances where the standards can/will not be implemented, the agency director must sign the Statewide Information Security Plan and Statewide Information Security Standards Deviation Report documenting compensating controls have been applied to adequately protect the information or acceptance of risk. This report must be kept on file for review by auditors or during a security assessment.

Section (3) – Standards Review: This standard will be reviewed at least every two years and updated as needed.