# Antivirus and Malware Policy

## Overview

The number of computer security incidents related to malware and viruses and the resulting cost of business disruption and service restoration continue to escalate. Implementing antimalware and antivirus systems, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are best practice actions that must be taken to reduce risks and manage the [LEP] computing environment.

## Purpose

The purpose of this policy is to describe requirements for preventing and addressing computer virus, worm, spyware, malware, and other types of malicious software.

## Scope

This policy applies to all [LEP] staff using [LEP] information resources.

## Policy

The [Insert Appropriate Role] or their designee shall ensure:

* Procedures and tools exist to guard against, detect, and report malicious software
* IT personnel are trained and proficient in the use of the security solutions used to protect against malicious software
* End users are aware of the security policies enforced on their workstations

### COMPUTING ASSETS

All workstation and server based assets used for state business, whether connected to the [LEP] network or as standalone units, must use [LEP] approved antivirus/antimalware protection software and configuration provided by the [LEP]. The following procedures shall be followed:

* Virus protection software must not be disabled or bypassed
* Settings for the virus protection software must not be altered in a manner that will reduce the software effectiveness
* Automatic update frequency cannot be altered to reduce the frequency of updates
* All servers attached to the [LEP] network must utilize [LEP] approved/standard virus protection software and setup to detect and clean viruses
* All electronic mail gateways, devices, and servers must use [LEP] approved e-mail virus/malware/spam protection software and must adhere to [LEP] rules for the setup and use of this software
* Any threat that is not automatically cleaned, quarantined, and subsequently deleted by malware protection software constitutes a security incident and must be reported to the IT Help Desk
* Antivirus/antimalware signature updates shall occur on a frequency defined by the [Insert Appropriate Role] but shall occur minimally once each calendar day

### APPLICATION INSTALLATION AND MANAGEMENT

All [LEP] authorized applications and software shall be installed by [Insert Appropriate Department] staff. [LEP] managed antivirus and malware software shall ensure:

* Authorized applications and software operate according to a clearly defined security policy
* All unauthorized applications and software are prevented from being executed.

### LICENSING, MAINTENANCE AND SUPPORT

Maintenance actions (software updates, definition updates, infections, etc.) shall be logged and retained for a period aligning with [Insert Appropriate Role] and [LEP] requirements to allow proper investigations into malware related incidents.

Management shall ensure proper licensing, tracking, and related documentation. This shall include processes and procedures supporting:

* Antivirus software installation on all systems
* Regular threat scanning capable of detecting, removing, and protecting against known types of malicious software
* Annual review and re-evaluation of low-risk systems and appliances not considered affected by malicious software based on current best practice
* Pro-active monitoring and update mechanisms supporting this policy
* Verification that mechanisms are in place for preventing users from disabling or modifying antivirus detection tools
* Processes and procedures for exceptions to the policy exist and are followed based on a case-by-case evaluation
* If antivirus mechanisms are disabled, additional security measures may need to be implemented for the period of time during which antivirus protection is not active.

## Audit Controls and Management

On-demand documented procedures and evidence of practices should be in place for this operational policy. Appropriate controls include:

* Virus and malware installation and update logs
* Associated virus scan and history logs
* Procedures for quarantine and removal of threats
* Documented remediation and communication procedures for large scale incidents

## VI. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## VII. Distribution

This policy is to be distributed to all [LEP] staff and contractors using [LEP] information resources.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 8/30/2016 | Policy Draft |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |