State of Vermont

Malicious Software Protection

Originally Approved: 11-02-10
Approved by: Tom Pelham
Policy Number:

Contents

1.0 Introduction

1.1 Authority

The State of Vermont is authorized to undertake the development of enterprise architecture policies and standards. The Department of Information and Innovation (DII) was created in VSA 22 § 901 (1), “to provide direction and oversight for all activities directly related to information technology, including telecommunications services, information technology equipment, software, accessibility, and networks in state government.”

Managers, employees, records personnel, third party vendors and all others who connect to or handle State of Vermont networks and data are responsible for reviewing this policy in concert with business, legal, and information technology staff to ensure that the policy (1) meets legal requirements specific to the agency and its data and (2) can be effectively carried out by agency employees. If laws or regulations require more stringent requirements than stated in this policy, the internal policy created by the agency must explicitly state the more stringent requirements. Agencies shall not develop an internal policy with requirements lower than the minimum requirements listed in this policy.

1.2 Purpose

For the purpose of this policy, department refers to any State entity including agencies, departments, boards and councils or other entities in the executive branch of government.

Anti-virus, anti-spyware and firewall software must be deployed on all workstations, portable computers, servers and other computing devices that attach to the State’s networks.

1.3 Scope

This policy applies to all agencies, departments, and other entitles including third-party business relationships that require access to non-public State resources. This includes, but is not limited to, desktop computers, laptop computers, proxy servers, mobile devices and any file and print servers. In addition, all e-mail gateway providers must provide malware checking and protection for email messages processed by the gateway.

Routine monitoring of networks can provide patterns of non-standard traffic that are indicative of many types of malware. If atypical traffic is detected, the IT staff of the Department of Information and Innovation (DII) will notify the agency/department of the

affected device. Departmental IT staff have authority to remove or disable any device producing suspicious traffic or with apparent virus infection and retain the equipment for investigation and/or forensic review, as needed. This includes 3rd party devices.

At their discretion, DII staff are empowered and encouraged to conduct audits of any PC systems that fall under this policy. This type of audit may be triggered when patterns of problems indicate that it is likely that associated standards for this policy are not being met.

2.0 Policy

Anti-malware applications will be used to protect the State of Vermont networks from malware infections and attacks. All desktop and laptop computers, servers and applicable devices must have current versions of software applications designed to detect malicious software.

Non-State equipment used in the conduct of State business through contractual or other agreements must be certified by the appropriate agency/department IT manager as having up-to-date anti-virus protection prior to allowing the device to assess the state networks. All individuals accessing State networks must not disable or disrupt the operation of anti-virus protection on any device. Nor should they in any way engage in practices that would introduce malicious software into the State's computing environment either directly or through data exchanges and transfers.

3.0 Policy Notification

Each state agency is responsible for ensuring that employees are aware of where policies are located on websites. Agencies are also responsible for notifying employees of policy change or the creation of new policies that pertain to the agency/department function.