

ITSec 5: ANTIVIRUS POLICY

Responsible Business Unit: IT
Affected Business Unit: All
Created by: Chris Pofahl

Creation Date: 1/03/2017
Effective Date: 3/2/2017
Expiration Date: [Expiration Date]

Introduction

Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans—enters the network during many business approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

Purpose

Requirement 5 of PCI DSS calls for businesses to Protect all systems against malware and regularly update anti-virus software or programs. This Policy Document addresses the antivirus section of the Vulnerability Management Program requirements of PCI DSS.

Scope

1. Policy Justification

- a. This Policy related document
- b. Additionally, this Policy related document insures the integrity, availability, and security of the City of Waukesha’s digital assets.

2. Affected Staff

- a. All City departments, offices, divisions, and agencies
- b. All represented and non-represented employees, contractors, and temporary workers

3. Significantly Related Documents and Policies

- a. ITFW-0.1 FIREWALL CONFIGURATION POLICY
- b. ITPW-0.1 SYSTEM AND PASSWORD POLICY
- c. ITSSD-0.1 STORING SENSITIVE DATA POLICY
- d. ITTSD-0.1 TRANSMISSION OF SENSITIVE DATA POLICY
- e. ITAV-0.1 ANTIVIRUS POLICY
- f. ITVS-0.1 VULNERABILITY SCANNING POLICY

4. Policy Maintenance

- a. Review this policy annually by Information Technology Board

5. Policy Statement

- a. All machines must be configured to run the latest anti-virus software as approved by the Company. The preferred application to use is XXXX



Anti-Virus software, which must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems.

- b. The antivirus software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits)
- c. All removable media (for example floppy and others) should be scanned for viruses before being used.
- d. All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements or at a minimum of PCI DSS requirement 10.7 of 3 months online and 1 year offline.
- e. Master Installations of the Antivirus software should be setup for automatic updates and periodic scans
- f. End users must not be able to modify any settings or alter the antivirus software
- g. E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

6. Enforcement

- a. Process Violation – See City of Waukesha HR Policy *B20 - Software Usage and Standardization* approved this 2nd day of February 2010.
- b. Additionally, see related regulation (governance, security, regulatory, HIPAA, SOX, ITIL, ISO, COBIT, PCI DSS, Homeland Security, State of Wisconsin, Federal Government, etc.) as applicable.

7. Standards Supporting this Policy

- a. PCI DSS
- b. **U.S. State Breach Notification Laws**
- c. **U.S. State Social Security Number Confidentiality Laws**
- d. **U.S. Patriot Act**
- e. **U.S. Federal Trade Commission (FTC) Consumer Rules**
- f. **U.S. Health Insurance Act (HIPAA).**

8. Procedures Enforcing this Policy

Approval

The Person(s) listed below approve this ITAV-0.1 Antivirus POLICY Approval guideline for IT use on the date specified.

Approver Name
[Approved by]

Approved On
[Approved]