|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Malicious Software Management Policy | | | | | |
| Policy # | CPL-11-05 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888-641-0500 |

Table of Contents

[Purpose 1](#_Toc457898835)

[Scope 1](#_Toc457898836)

[Policy 1](#_Toc457898837)

[Antivirus Deployment 1](#_Toc457898838)

[Antivirus Configuration 1](#_Toc457898839)

[Scanning Procedures 2](#_Toc457898840)

[Web Site Integrity 2](#_Toc457898841)

[Violations 2](#_Toc457898842)

[Definitions 3](#_Toc457898843)

[References 3](#_Toc457898844)

[Related Documents 3](#_Toc457898845)

[Approval and Ownership 3](#_Toc457898846)

[Revision History 4](#_Toc457898847)

Purpose

This policy defines the requirements for controls to prevent and detect the dissemination of any malicious software on Company X computer and communications systems.

Scope

This policy applies to all users of Company X computing, communications or information, including all employees, contractors, or temporary personnel.

Policy

### ****Antivirus Deployment****

**Antivirus Software Deployment** - Antivirus (anti-malware) software must be deployed and executing on all Company X computer and communications systems commonly affected by malicious software, e.g., personal computers and servers, where applicable anti-virus technology exists.

**Multiple Virus-Screening Packages** - At least two virus-screening software packages must be used at each point where electronic mail and other files enter the Company X network.

### ****Antivirus Configuration****

**Antivirus Software Updates** - All antivirus programs deployed on Company X computer and communications systems must be configured to accept automatic updates of the software.

**Antivirus Software Scans** - All antivirus programs deployed on Company X computer and communications systems must be configured to periodically scan all systems for malware.

**Antivirus Software Logs** - All antivirus programs deployed on Company X computer and communications systems must be configured to log all antivirus activity.

### ****Scanning Procedures****

**Downloaded Information** - All software and files downloaded from non-Company X sources through the Internet or any other public network must be screened with virus detection software prior to the software being executed or the files being examined through another program.

**Outbound Software And Executables** - All files containing software or executable statements must be certified as virus free prior to being sent to any third party.

**Decrypting Files For Virus Checking** - All externally-supplied computer-readable files must be decrypted prior to being subjected to an approved virus checking process.

**Scanning Remote Connections** - Company X must routinely scan the personal computers connected to its networks for viruses, worms, and Trojan horses, as well as to assure that users are employing only approved and licensed software.

**Electronic Mail Scanning And Footers** - All Company X mail servers must scan every inbound electronic mail message for viruses and personal message content, with a footer appended to each message stating that it has been scanned.

**Scanning Downloaded Software** - Before software downloaded from non-Company X sources is decompressed, it must be screened with an approved virus detection package after the user has logged off from all servers and terminated all other network connections.

**Scanning Backup Files For Viruses** - Before any files are restored to a production Company X computer system from backup storage media, these files must have been scanned with the latest version of virus screening software.

### ****Web Site Integrity****

**Regular Monitoring of Public Web Site for Malicious Software** - Company X must periodically perform a search of all public-facing internet computers for possible infection of malicious software.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Company X does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, Company X reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Definitions

**Antivirus Software** - A computer program designed to defend a computer system against malicious software, including viruses, Trojans, keystroke-loggers, hijackers, dialers, and other code that corrupts, damages or steals a computer system’s contents.

Confidential Information (Sensitive Information) – Any Company X information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by Company X from a third party under a non-disclosure agreement

**Malicious Software (Malware)** - [Software](http://www.webopedia.com/TERM/M/malware.html##) designed specifically to damage or disrupt a system, such as a [virus](http://www.webopedia.com/TERM/M/virus.html) or a [Trojan horse](http://www.webopedia.com/TERM/M/Trojan_horse.html).

Mobile Computing Devices - Mobile computing assets include, but are not limited to: laptop, notebook, tablet, desktop computers, all personal wireless-enabled devices, including pagers, cellular phones, mobile email devices, PDAs and other hybrid devices, and all portable storage media, including flash drives, smart cards, tokens, etc.

**Password** **–** An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

Partner – Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

**User -** Any Company X employee or partner who has been authorized to access any Company X electronic information resource.

References

CPL: 11.5 Malicious Software Protection

ISO/IEC 27002 - 12.2 Malware Protection

HIPAA: Integrity 164.312(c)(1)

HIPAA: Transmission Security- Integrity Controls (A)

PCI-DSS: R5. Use and regularly update anti-virus software or programs

Related Documents

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Contact | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | MM/DD/YYYY | MM/DD/YYYY |  |
|  |  |  |  |  |