Sample Protection against Malicious Programs Policy

Establishment date, effective date, and revision procedure

This policy was established and approved by [*Organization Name*] on mm,dd,yyyy, based on the Information Security Policy. The Information Security department of [*Organization Name*] shall review this policy at least once a year, and at any additional time when there are changes that may affect corporate management with respect to Information Security. In the event that amendment or repeal of this policy becomes necessary as a result of such review, the Information Security department of [*Organization Name*] shall prepare a draft and apply for authorization, and with prior confirmation of the Corporate Executive(s) in charge of the area(s) that will be affected by amendment or repeal. The [*Organization Name*] CISO/Security Director will authorize the amendment or repeal.

Table of revision history

Version	Date	Details of change	Issued by	Approved by

Introduction

Purpose

The purpose of this policy is to establish security requirements to be observed by [*Organization Name's*] IT Departments.

Scope

The scope of this policy shall be the same as the scope of [*Organization Name's*] Security Policy.

Applicability

This standard applies to the organization's Information System Corporate Executive and to all Information Systems personnel in the organization. If the applicable company does not have an IT department, this standard shall apply to the organization that has the equivalent function of the organization's IT department.

Definitions

The definitions shall be the same as those defined in the organization's Information Security Policy.

Protection from Malicious Code

Malicious Code is defined as all software that has been deliberately designed to harm or abuse the resources of computing systems. It is frequently concealed within, or masquerades as, legitimate software.

Malicious Code includes, but is not limited to, viruses, Trojan horses, worms, logic bombs, file infectors, malicious macros, malicious scripts (e.g. Java, ActiveX), malicious cookies, key loggers, and hidden software for launching denial-of-service attacks.

PCs and Portable Devices Protection from Malicious Code

The organization's IT Departments shall take appropriate measures to protect computers and portable devices against Malicious Code. Appropriate measures include:

- All information systems shall have installed the latest antivirus software that has been approved by the person in charge of Information Security.
- Where operationally possible, client PCs shall be protected by an automated process that maintains the latest versions of antivirus software.
- DAT files shall be updated automatically with the latest virus definitions immediately upon release.
- The entire storage area of the client PC shall be scanned at least once a week.
- Antivirus software shall be configured for real-time scanning of all information systems.
- Users shall not disable real-time scanning.
- Users shall report any suspected infection that has not been cleaned or quarantined to their IT Helpdesk and follow the instructions received.
- Antivirus administrators shall have a method to verify all client PCs have been updated with the latest version of DATs.
- Virus scanning software shall be set to automatically clean or delete infected files. If the virus scanning program is unable to clean/delete an infected file, the file that is infected shall be quarantined for further review by the administrators.
- All incoming Email and attachments shall be scanned for infections prior to being received at the user's inbox.

- All outgoing Email and attachments shall be scanned prior to leaving [*Organization Name's*] Email system.
- Personal Firewalls and Anti-Spyware shall be implemented in locations where network firewalls or IDS/IPS are not implemented, such as in small office implementations.

Server Protection from Malicious Code

[*Organization Name's*] IT Departments shall take appropriate measures to protect servers against Malicious Code. Appropriate measures include:

- Software and scripts residing on servers that facilitate the delivery of the automated antivirus process shall not be removed or edited without the approval of the person in charge of Information Security
- Continuously enabled approved virus checkers shall reside on all servers, where applicable
- Servers shall maintain the latest antivirus software
- The DAT file shall be distributed immediately upon release by the antivirus vendor