Important Note to User: This is a sample agreement and not "one-size-fits-all" and should not be used by any organization without review and modification to fit the needs of such organization. Organizations should cross-reference with relevant existing policies where appropriate, comparing against relevant policies (e.g. mobile device and acceptable use policies), ensuring terms are defined consistently across policies. Additional changes to this policy may be necessary to account for varying individual organizational security needs and user privacy expectations. In addition, while efforts have been made to ensure that the terms of this policy comply with employee rights under the National Labor Relations Act, this is a contentious and ever-changing area of the law, and therefore total compliance cannot be guaranteed. **Delete this note before publishing.**

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]. The [Organization Name] Information Security department 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 [Organization Name] Information Security department shall prepare a draft and apply for authorization, and with prior confirmation of the 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

Overview

Effective protection against malware is critical to protecting [Organization Name]'s sensitive information and information assets. The introduction of malicious software into the organization's system could result in significant losses including loss of sensitive information, inoperability, reputational harm, and potential legal exposures. As such, it is critical to preserve the integrity of organizational systems.

Purpose

The purpose of this policy is to establish the requirements for anti-malware and spyware protection on [Organization Name] Personal Computers (PCs) and servers.

Scope

This policy applies to employees, contractors, consultants, volunteers, temporary and other workers at [Organization Name], and all personnel affiliated with company subsidiaries or third parties. This policy applies to all equipment that is owned or leased by, or otherwise in the custody or control of, [Organization Name].

Policy

Malicious Software

Malicious software 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 software 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.

Protection of PCs and Portable Devices

The organization's IT Department shall take appropriate measures to protect computers and portable devices against malicious software. Appropriate measures include the following:

- All information systems should have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system. All anti-virus software must be approved by the Chief Information Officer [*or person of similar role within the organization*].
- Where operationally possible, organizational PCs should be protected by an automated process that maintains the latest versions of approved anti-virus software.
- DAT files should be automatically updated with the latest virus definitions immediately after their release.
- Organizational PCs should be scanned at least once a week.
- Users should report any suspected infection that has not been cleaned or quarantined to their IT Helpdesk and follow the instructions received.
- Antivirus administrators should verify that all organizational PCs have been updated with the latest version of DATs.

- Virus scanning software should 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 should be quarantined for further review by the administrators.
- All incoming and outgoing email and attachments should be scanned for infections prior to being received by the user or being sent from the organization's system.
- Personal firewalls and anti-spyware should be implemented where network firewalls or an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) are not implemented.
- All anti-virus applications must be updated as soon as patches, security fixes or any updates are available from the manufacturer. Maintaining up to date anti-virus software is critical to preserving the integrity of [*Organization Name*] systems.

Under no circumstances may any user disable anti-virus software or any of its processes without the express authorization of [Organization Name]'s IT department. IT personnel should supervise any disablement of anti-virus protection and such disablement should be for the shortest time possible to accomplish the needed objective.

Protection of Servers

[*Organization Name's*] IT Departments shall take appropriate measures to protect servers against malicious software. Appropriate measures include the following:

- All servers should have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system. All anti-virus software must be approved by the Chief Information Officer [*or person of similar role within the organization*].
- Servers should be protected by an automated process that maintains the latest versions of approved anti-virus software.
- Severs should be equipped with an IDS or IPS, where possible.
- The DAT file should be distributed immediately upon release by the antivirus vendor.
- Antivirus administrators should verify that all servers have been updated with the latest version of DATs.
- Virus scanning software should 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 should be quarantined for further review by the administrators.
- Mail servers should have either an external or internal anti-virus scanning application that scans all mail going to or coming from the mail server.
- Local anti-virus applications may be disabled during backups only where an external anti-virus application continues to scan inbound emails and network traffic while the backup is being performed.
- All anti-virus applications must be updated as soon as patches, security fixes or any updates are available from the manufacturer. Maintaining up to date anti-virus software is critical to preserving the integrity of [*Organization Name*] systems.

Policy Compliance

Compliance Measurement

Compliance with this policy will be verified by the [*Organization Name*] through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the [Policy Owner].

Exceptions

Any exception to the policy must be approved by the [Policy Owner] in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

By signing below, I acknowledge that I have read and fully understand my obligations under this Policy and hereby agree to abide by its terms.

______________________________	____________________
Name	Date