# Anti-Virus Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via email or instant messaging attachments, downloadable Internet files, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to [Company Name] in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of [Company Name] is to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by [Company Name] employees to help achieve effective virus detection and prevention.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This policy applies to all computers that are connected to the [Company Name] network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both company-owned computers and personally-owned computers attached to the [Company Name’s] network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. Currently, [Company Name] has [describe type of anti-virus software in use and type of license]. Licensed copies of [name anti-virus software] can be obtained at [online/offline location]. The most current available version of the anti-virus software package will be taken as the default standard.
2. All computers attached to the [Company Name’s] network must have standard, supported anti-virus software installed. This software must be active, scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.
3. Any activities with the intention to create and/or distribute malicious programs onto the [Company Name] network (e.g. viruses, worms, Trojan horses, email bombs, etc.) are strictly prohibited.
4. If an employee receives what he/she believes to be a virus or suspects that a computer is infected with a virus, it must be reported to the IT department immediately at [provide contact information]. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.
5. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT department.
6. Any virus-infected computer will be removed from the network until it is verified as virus-free.

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

1. Always run the standard anti-virus software provided by [Company Name].
2. Never open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source.
3. Never open any files or macros attached to an email from a known source (even a co-worker) if you were not expecting a specific attachment from that source.
4. Be suspicious of email messages containing links to unknown websites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
5. Files with the following filename extensions are blocked by the email system: [list extensions]. [Describe any workaround procedures for sending/receiving business-critical files with banned extensions, such as use of a file compression utility.]
6. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
7. Avoid direct portable drive (e.g. memory stick) sharing with read/write access. Always scan a portable drive for viruses before using it.
8. If instructed to delete email messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.
9. Back up critical data and systems configurations on a regular basis and store backups in a safe place.
10. Regularly update virus protection on personally-owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

The following activities are the responsibility of [Company Name] departments and employees:

1. Departments must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in this policy.
2. Departments that allow employees to use personally-owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.
3. All employees are responsible for taking reasonable measures to protect against virus infection.
4. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the [Company Name] network without the express consent of the IT department.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |