[INSERT FIRM LEGAL NAME]
Anti-Virus Management Policy

[Insert Firm Logo]

Version 1.0
[Insert Date]

This document is proprietary and confidential. The document and information contained herein may not be shared outside of [Insert Firm Legal Name] unless approved by authorized personnel.

Contents

Instructions 2

Policy Overview 2

Scope and Purpose 3

Compliance 4

Exceptions 4

Definitions and Terms 4

Appendix 5

Revision Table 5

Instructions

Documents are in a template format and are to be customized to fit the appropriate business and operational requirements. Use the sample as a foundation to build a bespoke policy for your business.

If any element of the following Sample/Template is not operationally feasible or appropriate for a particular business, be sure to delete that element from the company-specific document. **Otherwise, it would be a liability exposure to establish a policy and not to comply with it.**

The following recommendations are designed to limit, but will not eliminate, the security risks associated with the use of the policy subject. Businesses should deploy a defense-in-depth security model of technical, operational, and physical security controls.

Delete the instructions after finalizing and adopting the policy.

This document is enhanced using Human Intelligence (Hi) from the Riskigy vCISO team. For additional tuning and generating bespoke policies, procedures and plans the team can be reached at info@riskigy.com

Policy Overview

In order to protect the organization’s systems and data, we must minimize the amount of downtime to our systems and prevent risk to critical systems. This policy establishes prudent and acceptable practices regarding malware definitions, updates, and scanning.

Policy Detail

All computer devices connected to the network and networked resources shall have anti-virus software installed and configured so that the virus definition files are current and are routinely and automatically updated. The anti-virus software must be actively running on these devices. Virus scanning may be disabled when not in use but must be activated when the system is online.

Virus protection software must not be disabled or bypassed without IT approval.

The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

Virus protection software is required for each file server to protect the network from virus infections that could damage data, corrupt files, and compromise system integrity.

All email gateways must utilize IT-approved e-mail virus protection software. This software should regularly scan all files on computer devices for malware.

Any virus that is not scanned and automatically removed by such software constitutes a security incident and must be reported to the Service Desk.

If an infection is found on a computer device, the IT department reserves the right to disconnect that device from the network in order to prevent the propagation of the infection and associated detrimental effects.

Users:

- The fastest way to a virus is through an email attachment. Never open any unsolicited attachments attached to an email, regardless of where it was sent from. Do not download files or programs that you do not trust because they could contain viruses or other malicious code which can damage your computer.

- Delete spam, chain, and other junk mail without opening or forwarding the item. Spam is often disguised as legitimate email. Avoid replying to spam messages, forwarding them to colleagues, and clicking on links within those messages because it may expose your computer to viruses, Trojans, or other types of malware. In some cases, it will also prevent you from receiving legitimate emails.

- Never download files from unknown or suspicious sources.

- Always scan removable media from an unknown source (such as a CD or USB from a vendor) for viruses using a virus scanner before using it.

- Critical company data should be backed up on a regular basis and stored in a safe place. The IT Department will store the data on network drives and backup on a periodic basis.

Scope and Purpose

Scope

All computers connecting to the network for communications, file sharing, etc. are required to run anti-virus software at all times. All users are also responsible for downloading and installing updates for their anti-virus software. Failure to comply may result in loss of access to enterprise-level resources or other forms of disciplinary action.

Purpose

The following policy establishes the procedures and responsibilities related to the management of antivirus software. This policy is intended to help prevent the infection of computers, networks, and technology systems from malware and other malicious code.

Compliance

The Information Security team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Non-Compliance

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

Exceptions

Any exception to the policy must be approved by the Information Security team in advance.

Definitions and Terms

- **Virus**- A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from minimal to extremely destructive. A file virus executes when an infected file is accessed.

- **Worm**- a form of malware that spreads self-replicating copies of itself over computer networks. It does this by making copies of itself and sending them to others.

- **Spyware**- a type of malware that installs or runs without the knowledge and permission of the owner. These programs spy on your computer's activities and report them to their creator or third parties.

- **Trojan Horse**- programs that are malicious software and have been designed to look legitimate. They can be used to infect computers and compromise security. Trojan horse programs often appear in seemingly legitimate files, such as graphics, music, and games. Infected computers may also be exposed to other types of viruses and worms, which can result in a variety of problems including loss of data, disruption of services, and even damage to hardware if they are not caught at an early stage.

- **Malware**- a general term that refers to any software specifically designed to damage or disrupt computers and computer networks, or compromise their security. Malware can include viruses, worms, spyware, adware, and other malicious programs.

- **Ransomware**- a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files. Unless a ransom is paid, the malware typically won't let you operate your computer at all. Ransomware is on the rise because cyber criminals can make good money holding people's data hostage.

- **Adware**- software that is often spread without users' consent. Through the use of adware, advertisers can advertise their products or services through special pop-ups. Adware interrupts normal work smoothly and makes the system slow down or even freeze up.

Appendix

None

Revision Table

Revision History				
#	**Version #**	**Date**	**Updates/Changes**	**Owner**
1	1.0	2023	Initial Draft	Riskigy
2				