Antivirus and Anti-Malware Policy

[1. Purpose 2](#_Toc1707075510)

[2. Scope 3](#_Toc1709715753)

[3. Definitions 3](#_Toc1033527942)

[4. Policy 3](#_Toc1948841347)

[4.1. General Requirements 3](#_Toc1463081736)

[4.2. Remote Workers 4](#_Toc346906968)

[4.3. Incident Response 4](#_Toc611818135)

[4.4. Monitoring and Compliance 5](#_Toc1273888633)

[5. Roles and Responsibilities 5](#_Toc825442657)

[6. Enforcement 6](#_Toc1506068500)

[7. Review and Revision 6](#_Toc426018770)

[8. Document change control 6](#_Toc1401556638)

[Appendix A: List of Approved Antivirus and Anti-Malware Software 7](#_Toc2042155011)

[Appendix B: Incident Response Procedure 8](#_Toc907208667)

[Appendix C: Best Practices for Malware Prevention 9](#_Toc154193349)

[Appendix D: List of Common Malware Types 10](#_Toc1876561705)

# Purpose

The purpose of this policy is to establish guidelines and procedures for the effective use of antivirus and anti-malware software to protect the company’s information assets. This policy aims to minimize the risk of malware infections and ensure compliance with ISO/IEC 27001 standards for information security management.

# Scope

This policy applies to all employees, contractors, and third parties who access the company’s network, systems, and information assets. It includes all devices used for company business, whether company-owned or personal, especially considering that 80% of employees work remotely and use their personal devices.

# Definitions

* Antivirus Software: Software designed to detect, prevent, and remove malicious software (malware) such as viruses, worms, and trojans.
* Malware: Malicious software intended to damage or disable computers and computer systems.
* Personal Devices: Devices owned by employees or contractors and used for company business (e.g., laptops, tablets, smartphones).
* Full-Disk Encryption: Encryption technology that encrypts all data on a disk drive, ensuring that data is protected even if the device is lost or stolen.
* Incident Response: Actions taken to detect, respond to, and recover from a security incident, including malware infections.
* Virtual Private Network (VPN): A secure network connection over the internet that provides privacy and data security.

# Policy

## 4.1. General Requirements

* Installation and Activation: All devices used to access company networks and systems must have approved antivirus and anti-malware software installed, activated, and functioning at all times. Approved software must meet the company's security standards and be capable of detecting, preventing, and removing a wide range of malware.
* Regular Updates: The antivirus and anti-malware software must be configured to automatically update its virus definitions and perform regular scans to ensure up-to-date protection. The IT department will ensure that updates are applied promptly to protect against the latest threats.
* Scheduled Scans: Devices must be configured to perform full system scans at least once a week. Quick scans should be scheduled to run daily. These scans will help to detect and mitigate any potential threats.
* Immediate Reporting: Any detected malware must be reported to the IT department immediately, using the designated incident reporting procedures. The report should include details such as the type of malware, affected systems, and any observed symptoms.
* Approved Software List: The IT department is responsible for maintaining and updating a list of approved antivirus and anti-malware software. This list will be reviewed and updated regularly to ensure it includes the most effective solutions.
* Prohibited Actions: Employees must not install or use unapproved antivirus or anti-malware software on their devices. Additionally, employees are prohibited from disabling or bypassing any security controls installed on their devices. Unauthorized software can introduce vulnerabilities and compromise security.
* Network Controls: Network-level antivirus and anti-malware controls must be implemented to provide an additional layer of protection. This includes monitoring network traffic for malicious activity and blocking suspicious connections.

## 4.2. Remote Workers

* Compliance: Remote workers must ensure that their personal devices comply with this policy.
* Encryption: Personal devices used for company business must have full-disk encryption enabled to protect company data.
* Security Controls: Remote workers must not disable or bypass any security controls installed on their personal devices.
* Regular Maintenance: Remote workers must perform regular scans and updates as per the guidelines provided by the IT department.
* VPN Usage: Remote workers must connect to the company network using a secure Virtual Private Network (VPN) to ensure secure data transmission.
* Access Control: Remote workers must ensure that their personal devices are protected with strong passwords and, where possible, multi-factor authentication (MFA).
* Remote Desktop Services: When accessing company systems remotely, employees must use company-approved remote desktop services to ensure secure connections.
* Physical Security: Remote workers must ensure their personal devices are physically secure to prevent unauthorized access. This includes locking devices when not in use and avoiding use in public places where the screen can be viewed by others.

## 4.3. Incident Response

* Reporting: Any detected malware must be reported to the IT department immediately using the designated incident reporting procedures.
* Investigation: The IT department will investigate the reported malware incident and take appropriate action to contain and mitigate the threat.
* Containment: Devices found to be infected with malware may be disconnected from the company network until they are confirmed to be free of malware.
* Documentation: The IT department will document and review all malware incidents to improve future prevention measures and update the incident response plan as needed.
* Employee Cooperation: Employees must cooperate with the IT department during malware investigations and follow any instructions provided to remediate the threat.
* Recovery: Post-incident, the IT department will work to restore normal operations as quickly as possible while ensuring that all traces of malware have been removed. This may include restoring data from backups and re-imaging infected systems.
* Communication: In the event of a significant malware incident, the IT department will communicate with affected stakeholders, including employees, management, and potentially customers, to inform them of the incident and actions being taken.

## 4.4. Monitoring and Compliance

* Periodic Audits: The IT department will regularly monitor compliance with this policy through periodic audits and checks.
* Disciplinary Action: Non-compliance with this policy may result in disciplinary action, up to and including termination of employment. Contractors and third parties found in violation may have their contracts terminated.
* Training and Awareness: The IT department will provide regular training and awareness programs to ensure all employees understand the importance of this policy and their responsibilities.
* Monitoring Tools: The IT department will use monitoring tools to ensure that antivirus and anti-malware software is up-to-date and functioning correctly on all devices.
* Remediation Plans: The IT department will develop and implement remediation plans for any identified non-compliance issues.
* Reporting Metrics: The IT department will track and report on key metrics related to malware incidents and compliance, such as the number of detected threats, response times, and audit results, to management.

# 5. Roles and Responsibilities

* Employees: Ensure their devices comply with this policy, report any malware incidents immediately, and participate in training and awareness programs. Employees must also follow best practices for cybersecurity, such as avoiding suspicious links and attachments, using strong passwords, and maintaining device hygiene.
* Remote Workers: Follow additional guidelines for personal devices, perform regular updates and scans, ensure compliance with this policy, and use secure methods to access company resources. Remote workers must also ensure their home network is secure, including using a strong Wi-Fi password and keeping their router firmware up-to-date.
* IT Department: Maintain the list of approved antivirus and anti-malware software, provide support for installation and configuration, monitor compliance, respond to malware incidents, conduct training and awareness programs, and update this policy as needed. The IT department is also responsible for staying informed about the latest malware threats and updating defenses accordingly.
* Management: Ensure the policy is implemented effectively, provide necessary resources, enforce compliance, and support the IT department in maintaining security standards. Management must also promote a culture of security within the organization.
* Contractors and Third Parties: Ensure that any devices used to access company networks comply with this policy, report any security incidents to the IT department immediately, and follow the same security guidelines as employees. Contractors and third parties must also ensure that their own networks and systems are secure when accessing company resources.

# 6. Enforcement

Non-compliance with this policy may lead to disciplinary action, up to and including termination of employment. Contractors and third parties found in violation may have their contracts terminated. Additionally, repeated violations may result in loss of access to company networks and systems. The company reserves the right to take legal action against individuals or entities that violate this policy and cause harm to the company’s information assets.

# 7. Review and Revision

This policy will be reviewed annually and updated as necessary to ensure it remains effective and aligned with ISO/IEC 27001 standards. The review process will involve key stakeholders, including the IT department, management, and employee representatives.

# 8. Document change control

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Reviewed by | Reviewed Date | Reason to review | Approved by | Approved Date | Designation of the approver |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### Appendix A: List of Approved Antivirus and Anti-Malware Software

* Software 1: [Name, Version, Vendor]
* Software 2: [Name, Version, Vendor]
* Software 3: [Name, Version, Vendor]

### Appendix B: Incident Response Procedure

* Step 1: Detection and Reporting
  + Detect malware through antivirus software, user reports, or network monitoring tools.
  + Report the detected malware to the IT department immediately using the incident reporting system.
* Step 2: Initial Assessment
  + IT department assesses the severity and scope of the malware incident.
  + Determine whether to isolate affected systems to prevent further spread.
* Step 3: Containment
  + Disconnect infected devices from the network if necessary.
  + Implement temporary measures to contain the malware.
* Step 4: Eradication
  + Remove malware from infected systems using antivirus tools or manual methods.
  + Verify that all traces of the malware have been eradicated.
* Step 5: Recovery
  + Restore systems to normal operation, including data recovery if needed.
  + Conduct thorough testing to ensure systems are clean and fully functional.
* Step 6: Post-Incident Review
  + Documentation: Document the incident, including the type of malware, how it was detected, containment measures taken, and steps for eradication and recovery. Include any lessons learned and recommendations for improving security.
  + Review: Conduct a post-incident review to identify what worked well and what could be improved. Use this information to update the incident response plan and improve future responses.

### Appendix C: Best Practices for Malware Prevention

* Email Security: Be cautious when opening email attachments or clicking on links. Verify the sender's identity and scan attachments for malware before opening.
* Web Browsing: Avoid visiting suspicious websites or downloading files from untrusted sources. Use web filtering tools to block malicious sites.
* Software Updates: Keep all software, including operating systems and applications, up-to-date with the latest security patches.
* Strong Passwords: Use strong, unique passwords for all accounts and enable multi-factor authentication (MFA) where possible.
* Backup: Regularly back up important data to an external drive or cloud storage. Ensure backups are secure and not connected to the network during normal operations.
* Training: Participate in regular cybersecurity training and awareness programs to stay informed about the latest threats and best practices for prevention.
* Physical Security: Keep devices physically secure by locking them when not in use and avoiding use in public places where the screen can be viewed by others.

### Appendix D: List of Common Malware Types

* Viruses: Malicious programs that attach to other files and spread when the infected file is executed.
* Worms: Self-replicating malware that spreads across networks without human intervention.
* Trojans: Malicious programs disguised as legitimate software that grant unauthorized access to the system.
* Ransomware: Malware that encrypts data and demands payment for decryption.
* Spyware: Software that secretly monitors user activity and collects information without their knowledge.
* Adware: Unwanted software that displays advertisements and can track user behavior.
* Rootkits: Software that hides its presence and grants unauthorized access to the system.
* Keyloggers: Programs that record keystrokes to capture sensitive information, such as passwords and credit card numbers.