Antivirus Management Procedure

|  |  |
| --- | --- |
| Owner |  |
| Approver |  |
| Last Approved |  |

# Purpose

The document is established to protect the companyʼs electronic data, reduce the risk of data breaches, and safeguard the overall cybersecurity infrastructure by outlining the requirements and practices for effective antivirus management.

# Scope and applicability

This document applies to all company-owned devices and electronic data.

The document applies to all employees, contractors, and third-party stakeholders who use company resources.

# Roles and responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
| All users | Compliance with antivirus policy requirements.  Notifying IT of any observed or suspected malware issues. Participation in cyber security training. |
| Security and IT Teams | Implementing, maintaining, and updating anti-virus software on all relevant devices.  Conducting regular system scans and controlling automatic scan schedules. |

|  |  |
| --- | --- |
|  | Investigating received reports of potential malware. Recovery of damaged systems.  Keeping logs of virus detections and incident responses. |
| Director of Engineering, Security / Head of IT | Analyzes the cause of the incident, assesses the impact on information security, and coordinates the implementation of actions to prevent future malware incidents.  Approval and support of antivirus policy in the company. Allocating necessary resources to effectively manage the anti-virus program, including software funding, system upgrades, and staff training. |

1. **Antivirus management procedure**

## Antivirus software Installation and maintenance

All company systems, including corporate laptops must have the company- approved antivirus software installed.

This software shall not be altered or disabled without proper authorization and legitimate reason. The IT team is responsible for regular updates and patches to the software, ensuring optimal protection against known vulnerabilities.

## Regular scans and monitoring

Automated antivirus scans must be configured to run on all systems. The IT administrator monitors the results of these scans and performs additional manual scans when necessary, particularly in response to reported suspicions or detected threats.

## Incident response

### Detection and isolation

When a virus is detected, the antivirus system must immediately isolate the infected file to prevent further spread on the network.

Automatic notifications of the anti-virus system should be configured to notify the IT and Security team members about detected malware. Also, employees can

independently report such cases to [security@[Company Name].com.](mailto:security@sentry.com)

### Response

The response to a malware incident depends on the severity of the incident. The general classification of security incidents is defined in the Security Incident Management Procedure. But to determine the overall level of a malware incident, the following table is used:

|  |  |  |
| --- | --- | --- |
| **Incident criticality** | **Description and examples** | **Response** |
| Minor incidents | Description: Automatically detected and processed by antivirus software, have no impact on system performance or security.  Examples: Common viruses  and adware. | Response: Antivirus software automatically removes or blocks the threat without requiring the involvement of IT personnel.  Documentation: Not required. |
| Medium severity incidents | Description: Requires Security or IT staff involvement, may have minor impact on system performance or security.  Examples: Malicious software that requires manual intervention for complete removal; phishing attacks  requiring verification. | Response: Security or IT personnel intervene to remove the threat and restore the system.  Documentation: Not required |
| Major severity incidents | Description: Serious threats affecting performance, security, or data privacy.  Examples: Data leaks and large-scale attacks. | Response: Immediate intervention of IT or Security staff. It may be necessary to stop production processes and involve external specialists.  Documentation: Detailed documentation in Jira, including all stages of response, root cause analysis, and development of a plan to prevent similar incidents in the  future. |

To determine the criticality of the incident, the following criteria and questions should be used:

 **Impact on operations:** Does the incident disrupt regular system operations or business processes?

 **The prevalence of the threat:** Is the incident limited to one system, or does it spread across the network?

 **Data Loss:** Is there a risk of sensitive data being lost or compromised?

 **Recovery time:** What is the expected time to restore regular operations?

To respond to a malware incident, all or several items from the list below can be performed:

 **Isolation of an infected system:** Immediately disconnect the affected system from the network to prevent the spread of malware.

 **Using antivirus software** Analyze and remove malware using antivirus software.

 **Data recovery** Recover any corrupted or lost data from backups.

 **Incident analysis** Studying the causes and circumstances of an incident to avoid similar incidents in the future.

 **Software updates** Installing the latest security patches and updates for operating systems, antivirus software, and all other software involved. If necessary, updating outdated hardware that may present security risks.

 **Configuration verification:** Ensure all systems are configured correctly and securely, addressing known vulnerabilities.

If necessary, additional security measures may be implemented:

 **Layered security** Implementation of additional tools of a multi-layered security strategy, which includes firewalls, intrusion detection and prevention systems, cryptographic tools, etc.

 **Access restriction and privilege control** Establishing stricter access control policies, limiting user rights to the minimum necessary to perform their duties.

 **Regular auditing and monitoring** Implement systems to detect and respond to suspicious activity in real time. Carrying out periodic security audits.

 **Backup and recovery policies** Implement advanced backup and recovery policies to ensure disaster recovery without data loss.

 **Training and education of personnel** Continuous training of employees on cyber security issues, updating training programs given new threats and trends.

### Documentation

Incidents of high severity require documentation. To do this, a task in Jira should be created to record all information about the incident, its investigation, and response by the Incident Management Procedure.

# Malware types and response

To respond more effectively to the different types of malware that an organization may encounter; specific recommendations are provided for the main types of threats to detect, eliminate and prevent them:

|  |  |  |
| --- | --- | --- |
| **Malware type** | **Description** | **Response and prevention** |
| Viruses | Self-replicating programs that infect files to change or damage data. | Response: Using antivirus programs to detect and remove viruses. Restore damaged files from backups.  Prevention: Regular updates of antivirus software and operating systems. |
| Trojans | Malicious programs that masquerade as legitimate software to gain unauthorized access to the system. | Response: Identify and remove Trojans using antivirus software. Checking and cleaning the system.  Prevention: Do not download programs from unreliable sources or regular software updates. |
| Spyware | Programs that collect information about the user without their knowledge or consent, often for transmission to third parties. | Response: Using anti-virus and anti- spyware programs to detect and remove spyware.  Prevention: Be careful about downloadable files and the websites visited |

|  |  |  |
| --- | --- | --- |
| Adware | Programs that automatically display or download advertisements to the user's computer. | Response: Remove adware using antivirus software and clean browsers of unwanted extensions and toolbars.  Prevention: Avoiding unreliable downloads, using privacy and security settings in browsers, and regularly updating antivirus software. |
| Ransomware | Malware that blocks access to files or the system and demands a ransom for their recovery. | Response: Immediate disconnection from the network to prevent spread, use backups to restore data, and contact the IS manager.  Prevention: Regular data backup, software updates, and staff training to avoid suspicious links and attachments. |
| Worms | Self-replicating malware that spreads over a network without user interaction, often exploiting vulnerabilities in software. | Response: Using antivirus software to detect and remove worms and update and fix system vulnerabilities.  Prevention: Regular updating of software and operating systems, and use of firewalls to protect against unauthorized access. |

# User awareness

During annual security training, employees are regularly introduced to various cyber security threats and the importance of anti-virus protection as an integral component of our security measures. This ensures all employees know best practices and their role in maintaining the organization's security posture.

# Violation of the policy

Failure to comply with the antivirus policy may result in disciplinary action, including termination of employment or contract, legal action, or both. Any attempt to disable, bypass, or use anti-virus software will be considered a severe violation of company policy.

**History of the document**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Approval Date** | **Author** | **List of changes** | Approver |
|  |  |  |  |  |