**Anti-Malware/Anti-Virus Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_zb9ofo5ckyqn) **4**

[**Scope**](#_sebszm58trwj) **4**

[**Policy**](#_6mwzh76xs8yb) **4**

[**General statements**](#_9oonx8y6uo14) **4**

[**Logging and monitoring**](#_xifbmf2mm6cw) **4**

[**Remediation actions**](#_3pnnla4dgf4f) **5**

[**Testing**](#_9280ag1h7oaw) **5**

[**Disciplinary actions**](#_oo4pebgvtuk2) **5**

[**Change, Review, and Update**](#_6cu0cv3y3y7n) **5**

[**Responsibility**](#_fxvzxllev4xj) **5**

[**Reference**](#_abyh665p4kb0) **6**

[**Related Documents**](#_qfed4tf33320) **6**

# 

# Purpose

The purpose of this policy is to identify all controls associated with malware detection and make sure that these controls are set in place.

# Scope

This policy applies to all *[Company]* employees, contractors, third parties who access internal information and business processes.

# Policy

## General statements

* *[Company]* protects its internal/confidential information by detecting, preventing, and managing malware intrusions.
* Anti-malware security measures must be implemented to maintain the integrity, reliability, and performance of corporate systems.
* All IT systems connected to the network must run a supported version of the OS and installed applications with the latest available patches applied.
* All IT systems, including, but not limited to servers, desktops, laptops, must run the approved and supported anti-malware software packages.
* Anti-malware software shall be kept up to date.
* Users are restricted from disabling or removing the anti-malware software completely. All messages suggesting that anti-malware protection has been disabled have to be investigated immediately.
* Tamper protection must be enabled to prevent end-users or malware alerting software configuration or disabling the protection.
* The use of removable media is restricted and must be monitored.
* Users must be prevented from accessing known malicious websites either by malware protection software or through a content filtering function.
* An anti-malware product must scan email attachments before delivery.

## Logging and monitoring

* *[Company]* actively monitors (detection of known malware signatures, the endpoint being infected for a long time, etc.) network and IT systems connected to the network, including that activity, generated remotely.
* Anti-malware software shall be configured for real-time scanning and regularly scheduled scans. Anti-malware software conducts scans of critical computing devices on boot and at least every 24 hours.
* Malware signature updates shall be deployed across the network automatically.
* The scanning of IT equipment must be done before introducing it into the network.
* A log shall be kept of all scans undertaken; these logs should record as a minimum:
  + Date,
  + Time,
  + Address of area scanned,
  + Malware found,
  + Any action that was taken by the anti-malware software (e.g., quarantine or delete).

## Remediation actions

* In the case of violation of the business processes because of malware, the company has to recover from their effects as soon as possible.
* *[Company]* reserves the right to intercept and/or quarantine any network traffic or computing resources that may pose a threat to company infrastructure, systems, or data.
* The instance of the infection with malware sample(s) must be documented and raised as a security incident.
* The affected IT systems shouldn’t be active and be put into quarantine mode until they are malware-free.

## Testing

The anti-malware procedures must be periodically tested by deploying a safe and malicious-free file.

# Disciplinary actions

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Management will determine how severe an employee’s offense is and take the appropriate action.

# Change, Review, and Update

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by the ISMS Manager and approved by the ISMS Committee.

# Responsibility

This is the responsibility of the ISMS Manager to maintain and make sure everyone is aware of this policy.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# Related Documents

* Information Security Policy

# 

# 