**UnderDefense policy template kit**

Starting your compliance journey? UnderDefense policy template offers a comprehensive and compliance-ready document, complete with placeholders for company-specific details.

**How to use this document**

1. Thoroughly review the content of each policy, analyzing it section by section.
2. Evaluate whether the subsequent section and its associated risks are applicable to you. If it does not, remove it and/or replace it with your organization’s corresponding practices.
3. Replace any highlighted text in angled brackets < >[[1]](#footnote-0) with appropriate information (Use Find to make sure that all text in angled brackets is replaced)
4. Remove this instructions page
5. Add any company-specific letterhead, branding, and formatting
6. Save this document as PDF and upload to UnderDefenseMAXI to <https://app.underdefense.com/compliance/ISO27001/approved-policies>

# 

# **The Path to Compliance**

# We'll guide you through, ensuring a smooth path to compliance:



**SOC 2 Certification Timeline for SMBs with 50-250 Employees**

# 

# **Need Expert Assistance?**

| Navigating the complexities of compliance can be challenging, especially for businesses with limited internal resources or expertise.   * Experience team at the right time * Preparation of all compliance docs * Expert guidance on all tech-related issues   [**Book a call with expert**](https://meetings.hubspot.com/underdefense/help-with-compliance) | **Take your compliance from probable to guaranteed.** |
| --- | --- |

**<Your Company Logo>**

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

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 | <Date> | <Author> | Issued |
| 1.0 | <Date> | <Author> | Updated |
| 1.0 | <Date> | <Author> | Approved |
| **1.0** | <Date> | <Author> | **Granted “FINAL” status** |

| **Date of Next Revision** | **<date>** |
| --- | --- |

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

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

# ***Table of Contents***

[**The Path to Compliance 2**](#_htrkie77tuhx)

[**We'll guide you through, ensuring a smooth path to compliance: 2**](#_bor2nqthjwhg)

[**Need Expert Assistance? 2**](#_j1ad4z2lk78s)

[**Version Control Table 4**](#_1t3h5sf)

[**Table of Contents 5**](#_o5zm1vjf2d8f)

[**Purpose 6**](#_17dp8vu)

[**Scope 6**](#_3rdcrjn)

[**Responsibilities 6**](#_26in1rg)

[**Policy 6**](#_lnxbz9)

[General statements 6](#_35nkun2)

[Logging and monitoring 7](#_1ksv4uv)

[Remediation actions 7](#_44sinio)

[Testing 7](#_2jxsxqh)

[**Disciplinary actions 8**](#_z337ya)

[**Change, Review, and Update 8**](#_3j2qqm3)

[**Responsibility 8**](#_1y810tw)

[**Reference 8**](#_4i7ojhp)

[**Related Documents 8**](#_2xcytpi)

# 

# 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.

# Responsibilities

**ISMS Manager:**

* Manage anti-malware processes.
* Create documentation.

**SOC Analyst:**

* Monitor the activity associated with the malware infections and spreading;
* Prepare a report on critical information security incidents;
* Escalate true positive events to the Incident Management team.

**Incident Response Team:**

* Respond to the security incidents in time.

**Security Engineer:**

* Set up security configurations on the network equipment;
* Connect log sources with <SIEM>, and confirm the existence of alerts;
* Continuously improve the security system.

# 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.
* 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 deleting the anti-malware software. 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 by malware protection software or 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
  + Timу
  + 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 malware violation of the business processes, the company has to recover from their effects as soon as possible.
* <Company> reserves the right to intercept and quarantine any network traffic or computing resources that may threaten company infrastructure, systems, or data.
* 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

* ISO 27001 Annex A.12.2.1 Controls against malware

# Related Documents

* <Company> Risk Assessment

1. All fields in this document marked by angled brackets < > and highlighted must be filled in. [↑](#footnote-ref-0)