**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>**

**Software Installation Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 | <Date> | <Author> | Issued |
| 1.0 | <Date> | <Author> | Reviewed |
| 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**](#_arxqdy8knprl)

[**Table of Contents 5**](#_cj9vnfyr0ye6)

[**Purpose 6**](#_c09d0hpg606i)

[**Scope 6**](#_sebszm58trwj)

[**Responsibilities 6**](#_lfxpakk5qcyw)

[**Policy 6**](#_g3sfcv9793ai)

[Installation and support of software 6](#_xr2htx6z7x8c)

[Licensed software 7](#_mjherlh94yhd)

[Unlicensed software 7](#_9uvofi4m58u7)

[Unauthorized software 7](#_nalbf7qgsyyn)

[Exception 7](#_c0msidrqdlx5)

[**Disciplinary actions 8**](#_oo4pebgvtuk2)

[**Change, Review, and Update 8**](#_6cu0cv3y3y7n)

[**Responsibility 8**](#_fxvzxllev4xj)

[**Reference 8**](#_abyh665p4kb0)

[**Related Documents 8**](#_8mf7linb0n0o)

# 

# Purpose

The purpose of this policy is to identify all issues of the software installation processes. It is also created to minimize the risk of the exposure of sensitive information, unlicensed software exposure, and malware distribution.

# Scope

This policy applies to all <Company> employees, contractors, third parties who access internal information and business processes.

# Responsibilities

**ISMS Manager:**

1. Manage software installation process;
2. Create a list of all current software used in the company with SOC Analyst;
3. Create the Software Blacklist with SOC Analyst.

**SOC Analyst:**

1. Create a list of all current software used in the company with ISMS Manager;
2. Create the Software Blacklist with ISMS Manager;
3. Monitor the suspicious activity associated with the software installation;
4. Prepare a report on critical information security incidents;
5. Escalate actual true positive events to the Incident Management team.

**Incident Management Team:**

1. Respond to the security incidents in time.

**Security Engineer:**

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

# Policy

Employees have to refer to the <Company> Software Blocklist.

## Installation and support of software

The Asset Manager is exclusively responsible for installing and supporting all initial software on the corporate equipment. The Asset Manager relies on installation and support to provide software and hardware in good operating conditions to employees so they can best accomplish their tasks.

## Licensed software

It is the responsibility of the Asset Manager to ensure all licensing is accurate and up to date. To address this problem, Asset Manager is responsible for purchasing software licenses for the following software categories:

1. Desktop operating system software (Windows, Mac OS).
2. Productivity tools package (<VPN, EDR, etc.>).

The other software categories are the purchasing responsibility of the workgroup in which they serve. However, the application(s) are still installed and supported.

## Unlicensed software

1. Keep track of that if the software needs a license. Many applications can be installed only in case of paying the initial/monthly/annual fee. The exception is, of course, the “freeware” or “public domain software.”
2. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period.
3. Some software is limited to free use by private individuals, whereas commercial use requires a license payment, so do not risk bringing <Company> into disrepute by breaking the law.

## Unauthorized software

1. Employees can install software on corporate equipment only for professional usage.
2. It is restricted to downloading, installing, or using unauthorized software because it can cause severe hardware and network security vulnerabilities.
3. Software packages that permit the computer to be ‘remote-controlled’ (e.g., PC anywhere), ‘hacking tools’ (e.g., network sniffers and password crackers), and any kind of not corporate VPN are explicitly forbidden on equipment unless they have been pre-authorized expressly by management for legitimate business purposes.

## Exception

1. Pentester Team is allowed to install malicious or any type of software or files as a part of their work only on virtual machines or using an isolated network provided by <Company>.

# 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.12.5.1 Installation of software on operational systems
* ISO 27001 Annex A.12.6.2 Restrictions on software installation
* ISO 27001 Annex A.18.1.2 Intellectual property rights

# Related Documents

* <Company> Risk Assessment

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