**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>**

**Removable Media 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>** |
| --- | --- |

# 

# ***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**](#_9z7um3g4c50a)

[**Table of Contents 5**](#_lw6p71bg2dbk)

[**Purpose 5**](#_lx7cfhno89u9)

[**Scope 6**](#_l724r1z428ud)

[**Policy 6**](#_cbra7c4n9gl8)

[**Disciplinary actions 6**](#_oo4pebgvtuk2)

[**Change, Review, and Update 6**](#_6cu0cv3y3y7n)

[**Responsibility 6**](#_fxvzxllev4xj)

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

[**Related Documents 6**](#_ukche8hbs94u)

[**Procedures & Implementation best practices 6**](#_ezxgbvcrdpof)

# 

# Purpose

This policy describes the way we see using any type of removable media in our company. The purpose is to minimize the risk of loss or exposure of the company’s information maintained by <Company>.

# Scope

This policy applies to all employees, users, and third parties who access or use <Company> information assets, regardless of physical location.

IT resources include all company-owned, licensed, leased, or managed hardware and software used by the <Company> Infosec network via a physical or wireless connection, regardless of the ownership of the computing device connected to the network.

# Policy

* Removable media usage is strictly prohibited (except if it is explicitly allowed by the Management), as it poses a high risk of malware infections or corporate data loss.
* The only way of the applied data transfer is <Defined resource>. Employees cannot download any type of received data on the USB drive or any other removable media.
* The exception is Asset Manager, who can sometimes use the approved USB Drive for installation purposes.
* Employees can ask for individual exceptions from the Management.

# 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.8.3.1 Management of Removable Media

# Related Documents

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