**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>**

**Bring Your Own Device 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**](#_59iexwsaii4u)

[**Purpose 6**](#_ey50fsgrk2rg)

[**Scope 6**](#_65t2t559434o)

[**Policy 6**](#_16mxz7su9rxh)

[Laptops 6](#_tyjcwt)

[Mobile devices 7](#_u2an8rst0pnx)

[**Disciplinary actions 7**](#_oo4pebgvtuk2)

[**Change, Review, and Update 7**](#_6cu0cv3y3y7n)

[**Responsibility 7**](#_fxvzxllev4xj)

[**Reference 8**](#_1ksv4uv)

[**Related Documents 8**](#_oqj2g9kzbmil)

# 

# Purpose

This document defines the security rules and controls required when working with not organization-owned devices inside the <Company> office/network infrastructure. It serves as a central policy document with which all employees and contractors must be familiar and defines actions that all users must follow.

The purpose of this Bring Your Own Device Policy is to provide a comprehensive framework for:

* Ensuring the confidentiality, integrity, and availability of <Company> employees’ PII information.
* Ensuring the confidentiality, integrity, and availability of <Company> trusted parties’ information.
* Ensuring security and integrity of <Company> internal infrastructure.
* Protection from unintentional sensitive data leakage.

# Scope

This policy applies to all employees, users, and third parties who access or use <Company> internal infrastructure.

Resources under the scope of this policy include all not company-owned devices entering the territory of the <Company> office or connecting to the <Company> internal network infrastructure.

# Policy

## Laptops

* <Company> Guest’s network is provided for connections from non-company-owned devices.
* Non-company-owned laptops are prohibited from being used inside the <Company> office. But in case if: (a) The company-owned device was not assigned to an employee or contractor due to security reasons; (b) The company-owned device was not assigned to an employee or contractor due to a temporary contract bearing in mind a short-term task without further cooperation; (c) The company-owned device was not assigned to an employee or contractor due to complications by unexpected troubles in transportation or assignment circumstances.
* Non-company-owned device that meets requirements described below can be used for business purposes:
  + Full corporate security package must be installed on a device.

1. EDR agents.
2. MDM agents.
3. Disk encryption (Linux - Full disk encryption while OS installation; MacOS - FileVault; Windows - BitLocker).
4. SIEM forwarder.
   * Strong device authentication is implemented according to the <Company> Password Management Policy.
   * Corporate environment must be properly separated from the personal one.

* A non-company-owned device can be used but only while connected to the <Company> Guest network
* It is prohibited to connect to the internal <Company> InfoSec network infrastructure from a non-company-owned device.
* It is prohibited to keep any <Company> company and client-related documentation on a non-company-owned device, these documents and information must be stored on corporate Google Drive or other approved cloud storages.
* It is prohibited to install on laptop software from the <Company> Software Blocklist, except for licensed games and messengers from trusted sources.

## Mobile devices

* Personal mobile devices are not prohibited from using inside the <Company> office while connected to the <Company> Guest network.
* It is prohibited to download any company’s or client-related data on personal mobile devices.

# 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 A.6 Controls about rules of using non-company-owned devices

# Related Documents

* <Company> Acceptable Use Policy
* <Company> Asset Management Policy
* <Company> Password Management
* <Company> Remote Access Policy

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