**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>**

**Clear Desk and Clear Screen 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**](#_ukruovgntws6)

[**Purpose 6**](#_c1g4bgtkjdjs)

[**Scope 6**](#_3dy6vkm)

[**Policy 6**](#_1t3h5sf)

[Clear Desk Policy 6](#_3rdcrjn)

[Clear Screen Policy 6](#_k0ow78rxp1qv)

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

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

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

[**Reference 7**](#_1ksv4uv)

[**Related Documents 7**](#_oqj2g9kzbmil)

# 

# Purpose

The purpose of this policy is to establish the minimum requirements for maintaining clean desks and clear screens and to ensure that where there is any confidential, restricted, or sensitive Information that is locked away and is out of sight.

# Scope

This policy applies to all employees, contractors, subcontractors, consultants, temporaries, guests, and any third party that uses <Company> information assets or information resources and services.

# Policy

## Clear Desk Policy

1. Hard copy documents containing any personal data or confidential, restricted, or sensitive information should only be stored safely. Examples are contracts with clients, contractors, employees and NDA.
2. Prefer to use digital versions of documents instead of printed copies.
3. Any confidential, restricted, or sensitive information must be removed from desks and locked in a drawer when a desk is left unoccupied at any time.
4. Keys for the server room must not be left in or on an unattended desk. The keys’ owner is responsible for keeping them safe.
5. No confidential information must be left in meeting rooms, either on the table, slides, or on whiteboards.
6. Passwords must not be left on sticky notes posted on or under a computer or written down and left in an accessible location.
7. Any information sent to printers should be retrieved as soon as practicable.

## Clear Screen Policy

1. When leaving their desks for any period, staff must ensure that they lock their computer to prevent unauthorized access to information or systems.
2. Lock your screen when you leave your computer unattended:
   * For Windows devices: Press Ctrl, Alt, and Delete keys simultaneously and then ENTER or Press the Windows button (between the Ctrl and Alt keys) on your keyboard and L simultaneously
   * For macOS running macOS Mojave: go to the Apple menu and choose Lock Screen or press Command+Control+Q. This will lock your Mac and return you to the Login screen.
   * For macOS running an earlier operating system: press the Control+Shift+Power button (or Control+Shift+Eject if your Mac has an optical drive). It will lock the screen.
   * For Linux - Ctrl+Alt+L or Super+L (i.e., holding down the Windows key and pressing L) should work. Once your screen is locked, you will have to enter your password to log back in.
3. Computer workstations must be logged off at the end of the working day to install security updates during the evening.
4. Screensavers and computer timeouts must be password protected.
5. All computer screensavers should be set for a maximum of five (5) minutes to lock, requiring a password to re-enter the computer.
6. Keeping 4 and 5 items (above) of security configuration on the user workstation is the contractor and employees' responsibility.

# 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 or employee that was specifically appointed to perform such a task by 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.11.2.9 Clear Desk & Screen Policy

# Related Documents

* <Company> Physical Security Policy

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