**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>**

**Physical Security 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 1**](#_htrkie77tuhx)

[**We'll guide you through, ensuring a smooth path to compliance: 1**](#_bor2nqthjwhg)

[**Need Expert Assistance? 1**](#_j1ad4z2lk78s)

[**Version Control Table 3**](#_arxqdy8knprl)

[**Table of Contents 4**](#_y95gth64v02r)

[**Purpose 4**](#_c1g4bgtkjdjs)

[**Scope 4**](#_3dy6vkm)

[**Policy 5**](#_1t3h5sf)

[Physical Data Security 5](#_n7jjsvh33gbe)

[Physical Security Policy 5](#_3rdcrjn)

[Physical System Security 6](#_hwj159upsg6k)

[Fire Prevention 6](#_cppk6p1m5d4d)

[Access to the office 7](#_gbne1cz46iu3)

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

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

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

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

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

# 

# 

# Purpose

This policy aims to establish the rules for granting control, monitoring, and removing physical access to office premises; to identify sensitive areas within the organization.

# 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

## Physical Data Security

Certain physical precautions must be taken to ensure the integrity of the company’s data. At a minimum, the following guidelines must be followed:

1. Users must follow Clear Desk and Clear Screen Policy.
2. Network cabling should not run through unsecured areas.
3. Information systems and their components shall be positioned within the facility to minimize risks from physical and environmental hazards and opportunities for unauthorized access.

## Physical Security Policy

1. A responsible person (COO) controls physical security in <Company>.
2. Access cards shall be issued and fingerprints shall be registered in the door lock system to all employees.
3. Access cards and fingerprints, for the door lock system to every employee, shall be revoked in case of dismissal.
4. Any equipment/IT assets considered “Critical” shall be protected from environmental threats, hazards, and unauthorized access.
5. Any incidents related to physical security breaches resulting in unauthorized access shall be reported to the responsible person (COO).
6. In the case of a power outage, the automatic door system will continue working from a reserve power source for at least 12 hours. After discharge of the reserve battery door should be closed manually by a responsible person (COO).
7. The power, telecommunication, and data cabling shall be protected wherever possible from interceptions and damages.
8. The equipment shall be maintained at least annually to ensure its continuous availability and integrity.
9. All the equipment to be taken off-site needs written permission from the management.
10. Any storage device (USB-sticks, CDs, HDD, SSD drives, etc.) shall be checked to ensure that any company data and licensed software on it are securely purged before disposal.
11. All critical documentation must be destroyed through a shredder before being thrown into the general trash.
12. CCTV is present near the office entrance.
13. Critical backup media shall be kept in a fireproof off-site location in a vault.
14. Information systems and their components shall be positioned within the facility to minimize risks from physical and environmental hazards and opportunities for unauthorized access.
15. Physical protection against damage from fire, flood, civil unrest, and other forms of natural and man-made disasters shall be designed and applied.
16. All statements stated above shall be monitored for any changes at least annually.

## Physical System Security

In addition to protecting the data on the company’s information technology assets, this policy provides the guidelines below on keeping the systems themselves secure from damage.

Systems that store company data are often sensitive electronic devices that are susceptible to being inadvertently damaged. To minimize the risk of damage, the following guidelines must be followed:

Minimizing Risk of Damage

1. Environmental controls should keep the operating environment of company systems within standards specified by the manufacturer.
2. Proper grounding procedures must be followed.
3. Strong magnets must not be used in proximity to company systems or media.
4. Except in a fire suppression system, open liquids must not be located above company systems. Technicians working on or near company systems should never use the systems as tables for beverages.
5. UPS is required for important systems and encouraged for all systems.

## Fire Prevention

It is the company’s policy to provide a safe workplace that minimizes the risk of fire.

1. Fire, smoke alarms, and suppression systems must be used and conform to local fire codes and applicable ordinances.
2. Electrical outlets must not be overloaded. Users must not chain multiple power strips, extension cords, or surge protectors together.
3. If possible, unused electrical equipment should be turned off when not in use for extended periods (i.e., during non-business hours).
4. If overly worn equipment is found, the equipment must be replaced or taken out of service immediately, depending on the degree of wear.
5. A smoke alarm monitoring system is our office landlord’s responsibility.
6. In case of evacuation follow the office evacuation plan.
7. Trash/waste is properly stowed in trash/recycling bins, not piled up in any area, especially doorways.

## Access to the office

1. All employees’ entries are recorded on the CCTV, and data is gathered from the door lock system.
2. All employees are required to use their cards or/and fingerprints when entering the office.
3. Employees are forbidden from leaving their access cards unattended.
4. Employees must inform the HR Generalist in the event of an access card loss.
5. All new hires are required to wear a badge for the first month of their employment.
6. Outside visitors must be accompanied by someone from the <Company> only. This person is responsible for visitors’ abidance with the company’s rules.
7. Each visitor is recorded in the <Company> Visitor Log Spreadsheet by the person who accompanies the visitor.
8. The COO, HR Generalist and Office Manager are fully responsible for managing access to the office. Office Manager is responsible for maintaining the Visitor Log Spreadsheet.
9. Once a month, the visitor activity is reviewed by the Office Manager.
10. Office is a private place and each visitor must follow the photo and videography restrictions policies:
    * Do not take photos or videos of an employee’s workplace.
    * Do not take photos or videos of employees without their agreement.
    * Do not take photos or videos of any confidential information.
    * Visitors can take pictures with the consent of 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 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.11.1.1 Physical Security Perimeter
* ISO 27001 A.11.1.2 Physical Entry Controls
* ISO 27001 A.11.1.3 Securing Offices, Rooms, and Facilities
* ISO 27001 A.11.1.4 Protecting against External & Environmental Threats
* ISO 27001 A.11.1.5 Working in Secure Areas

# Related Documents

* <Company> Clear Desk and Clear Screen Policy
* <Company> Incident Response Plan
* <Company> Employee Handbook
* <Company> Acceptable Use Policy
* <Company> ISMS Manual

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