**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>**

**Access Management 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**](#_7oqfmz9ribbc)

[**Table of Contents 5**](#_xxo923m8zwcm)

[**Purpose 6**](#_17dp8vu)

[**Scope 6**](#_3rdcrjn)

[**Policy 6**](#_26in1rg)

[General rules for Access Management 6](#_lnxbz9)

[Access to Network and Network Services 6](#_35nkun2)

[User Registration and Deregistration 6](#_1ksv4uv)

[User Access Provisioning 7](#_44sinio)

[Management of Privileged Access Rights 7](#_2jxsxqh)

[Review of User Access Rights 7](#_z337ya)

[Workstation Lockout 7](#_3j2qqm3)

[Password Management 8](#_rhn4t2mkv2hw)

[**Disciplinary actions 8**](#_4i7ojhp)

[**Change, Review, and Update 8**](#_2xcytpi)

[**Responsibility 8**](#_1ci93xb)

[**Reference 8**](#_3whwml4)

[**Related Documents 8**](#_2bn6wsx)

[**Procedures & Implementation best practices 9**](#_ezxgbvcrdpof)

# 

# 

# Purpose

<Company> is committed to the correct use and management of access controls throughout the organization. The purpose of this policy is to define the steps that must be taken to ensure that users connecting to <Company> resources are authenticated appropriately, in compliance with company standards, and are given the least amount of access required to perform their job function.

# Scope

The scope of this policy includes all users who have access to company-owned or company-provided computers or require access to the corporate network and systems. This policy applies to employees and guests, contractors, and anyone needing access to the corporate systems.

# Policy

## General rules for Access Management

* All <Company> information systems must be password protected.
* All <Company> information systems must be MFA protected where possible.
* All <Company> information systems must be accessible only through Corporate VPN when protection by MFA is impossible.
* All <Company> information systems must have a designated information owner responsible for managing and controlling access to the system.
* All <Company> information systems must have a designated system administrator. For some systems, it can be its owner as well.
* Access to all <Company> information systems and networks must be strictly controlled by formal registration and deregistration processes.
* Access to all <Company> information systems must be controlled by using unique user accounts.
* Regular access review process is performed to the critical systems only (<List of critical systems, Google Workspace etc.>).

## Access to Network and Network Services

* Only authorized personnel have access to the network services, where they will manage other necessary accesses, create, review, backup, and change network services configurations.

## User Registration and Deregistration

* All company employees must have their unique user account to serve as an identifier for their different systems, including the information that can identify them.
* Usage of an outdated user account is prohibited.
* Usage of one user account by different employees is unacceptable.
* Sharing the credentials with another employee or person not working in <Company> is prohibited.
* Security Engineer creates new user accounts only after receiving the official requests.
* Security Engineer creates a new user or role using the user account as a name.
* When an employee leaves <Company>, all their information systems, network, and project-based accesses must be revoked as soon as possible. The access revoking is approved by the PM and done by a Security Engineer.

## User Access Provisioning

* Requests from users for password resets must only be performed when the Security Engineer has verified the employee’s identity.
* Existing users who require additional access privileges must make the official written request.
* Accesses for users who change their work responsibilities must be reviewed to ensure that the new role will not require those accesses. If the access is not needed, it will be revoked.

## Management of Privileged Access Rights

* Access rights and privileges to <Company> information systems must be allocated based on the user’s functions.
* The principles of zero-trust, least privilege, and need-to-know must be followed.
* Access privileges granted to users must not undermine essential segregation of duties.
* The creation of user access accounts with special privileges, such as administrators, must be controlled and restricted to only those responsible for managing or maintaining the information systems.

## Review of User Access Rights

* System administrators (owners) must conduct a quarterly review of the access rights for critical systems.

## Workstation Lockout

* <Company> employees must lock their workstations in case of inactivity and re-enter the password.

For more information, refer to the <Company> Clear Desk and Clear Screen Policy.

## 

## Password Management

* The employees are required to follow the rules for maintaining passwords securely.

For more information, refer to the <Company> Password Management Policy.

# 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.9.1.1 Access Control Policy
* ISO 27001 Annex A.9.1.2 Access to Networks and Network Services
* ISO 27001 Annex A.9.2.1 User Registration and Deregistration
* ISO 27001 Annex A.9.2.2 User Access Provisioning
* ISO 27001 Annex A.9.2.3 Management of Privileged Access Rights
* ISO 27001 Annex A.9.2.4 Management of Secret Authentication Information of User
* ISO 27001 Annex A.9.2.5 Review of User Access Rights
* ISO 27001 Annex A.9.2.6 Removal or Adjustment of Access Rights
* ISO 27001 Annex A.9.3.1 Use of Secret Authentication Information
* ISO 27001 Annex A.9.4.1 Information Access Restriction
* ISO 27001 Annex A.9.4.2 Secure log-on Procedures
* ISO 27001 Annex A.9.4.3 Password Management System
* ISO 27001 Annex A.9.4.4 Use of Privileged Utility Programmes

# Related Documents

* <Company> Password Management Policy
* <Company> Clear Desk and Screen Policy

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