**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>**

**Remote Access 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 thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarize the change and 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**](#_1t3h5sf)

[**Table of Contents 5**](#_2s8eyo1)

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

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

[**Policy 6**](#_lnxbz9)

[Prohibited Actions 6](#_35nkun2)

[Network Access 6](#_1ksv4uv)

[**Disciplinary actions 7**](#_2jxsxqh)

[**Change, Review, and Update 7**](#_z337ya)

[**Responsibility 7**](#_3j2qqm3)

[**Reference 7**](#_1y810tw)

[**Related Documents 7**](#_4i7ojhp)

# 

# Purpose

This policy is provided to define standards for accessing corporate information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc.

# 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

## Prohibited Actions

Remote access to corporate systems is only to be offered through a company-provided means of remote access in a secure fashion. The following are specifically prohibited:

* Installing any remote access devices on a company system without approval.
* Remotely accessing corporate systems with the remote desktop tools without approval.
* Use of non-company-provided remote access software.

## Network Access

* There are no restrictions on what information or network segments users can access when working remotely, however, the level of access should not exceed the access a user receives when working in the office.
* Working with clients information should be performed through VPN only in order to protect the data from malicious scenarios.

Currently <Company> uses <Firewall> to provide employees remote network access. The VPN relies on the TLS protocol and is segregated into several purpose subconnections:

* Engineers and developers
* Sales and Marketing
* Management
* SOC Analytics

In order to add an additional layer of security MFA is configured for accessing VPN profiles.

The usage instruction is available for all employees and contractors of <Company>.

# 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.9.1.1 Access Control

# Related Documents

* <Company> Password Management Policy

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