**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>**

**Information 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 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)

[**Table of Contents 4**](#_yva7houuftia)

[**Purpose 6**](#_133esk9ywqc)

[**Scope 6**](#_5asa0pjtdse8)

[**Policy 6**](#_888fwa3khkjs)

[Communication Security 7](#_lkwnh4y7zvst)

[Data Classification 7](#_u8dvps4y0o8x)

[Security Awareness 7](#_wl4wh4v0km8q)

[Prohibited Activities 7](#_ha7iossi3rtv)

[**Disciplinary actions 8**](#_oo4pebgvtuk2)

[**Change, Review, and Update 8**](#_6cu0cv3y3y7n)

[**Responsibility 8**](#_fxvzxllev4xj)

[**Reference 8**](#_u3w124gxb1xn)

[**Related Documents 8**](#_aibf5kep9lx3)

[**Procedures & Implementation best practices 8**](#_ezxgbvcrdpof)

# 

# 

# Purpose

This document defines the technical controls and security configurations required to ensure the integrity and availability of the data environment at <Company>. 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 Information Security Policy is to provide a comprehensive framework for:

* Protecting the confidentiality, integrity, and availability of <Company> assets.
* Protecting <Company>, its employees, and clients from the illicit use of <Company’s> information assets and information resources.
* Ensuring the effectiveness of information security controls over information assets and information resources that support <Company> operations.
* Ensuring that regular review of this manual is conducted at a minimum annually or more frequently as needed.

# Scope

This policy applies to all employees, users, and third parties who access or use <Company> information assets, regardless of physical location.

IT resources include all company-owned, licensed, leased, or managed hardware and software and use the <Company> network via a physical or wireless connection, regardless of the ownership of the computing device connected to the network.

# Policy

* The Information Security Policy is a master document for all policies and procedures established in the company.
* All other policies aim to support this policy in describing requirements and processes and setting definite rules for supporting a strong level of Information Security.
* Each policy has an owner who is responsible for:
  + Ensuring that it is kept up-to-date.
  + Ensuring that it is understandable and reflects the current state of information security.
  + Ensuring that it is communicated to all employees.
* Policies and procedures are reviewed annually or in case of change and approved by the ISMS Committee.
* All ISMS documentation is stored in the <Company> ISMS folder, and people responsible for ISMS implementation maintain this folder up-to-date.
* All ISMS documentation is shared with employees on <Company’s internal informational resource>.

## Communication Security

* Employees must use only approved ways for communication: corporate Google Workspace email, Google Chat, or other for corporate use only.
* Employees are not allowed to use corporate email for personal communication.
* Employees should not open any attachments from the unknown senders or when received unexpectedly.

For more information on this topic, refer to <Company> Acceptable Use Policy.

## Data Classification

Here are some recommendations for securing confidential information:

* Do not disclose the confidential data without proper authorization and ensure that person has the NDA signed with <Company>.
* Do not download any company’s data on your personal device.
* Lock or secure, confidential paper documents at all times.
* Destroy confidential documents when they’re no longer needed.
* Encrypt electronic data.
* Make sure employees view confidential data on secure devices.
* Avoid transferring sensitive data to other devices or accounts unless necessary.
* Ensure that the recipients of transferred sensitive data are properly authorized people and respective organizations have adequate security policies.
* Return any confidential data and delete it from personal devices (where applicable) when employees stop working for our company.
* Employees should not:
  + Use confidential information for any personal benefit or profit.
  + Replicate confidential data and store it on insecure devices.

For more information on Data Classification, refer to <Company> Data Classification Policy.

## Security Awareness

Employees are obligated to participate in the Securing Awareness training sessions before employment and annually after that. The training material is selected by the ISMS Manager and approved by the ISMS Committee. The understanding of given material is checked in the form of a Questionnaire.

## Prohibited Activities

Personnel is prohibited from the activities that are referenced in all other sub-policies - <Company> ISMS policies.

# 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.5.1.1 Policies for Information Security
* ISO 27001 Annex A.5.1.2 Review of the policies for information security

# Related Documents

* <Company> ISMS Manual
* <Company> Acceptable Use Policy

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