**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>**

**Backup Policy**

# 

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 | <Date> | <Author> | Issued |
| 1.0 | <Date> | <Author> | Updated |
| 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**](#_acsm13oho249)

[**Table of Contents 5**](#_ukruovgntws6)

[**Purpose 5**](#_67i62vthxmjc)

[**Scope 5**](#_sebszm58trwj)

[**Responsibilities 6**](#_1cibex4010ah)

[**Policy 6**](#_5rj02xnd3hsl)

[Information backup 6](#_5pm7n5y25pd2)

[Timing 7](#_99fv2rmh4ohy)

[Testing 7](#_1vryqmwmfit7)

[Storage 7](#_jzx8fyyws11)

[Retention period 7](#_qfg8bf4wu78f)

[**Disciplinary actions 7**](#_tfm2t62n6ro)

[**Change, Review, and Update 7**](#_gfxmghp2iiwl)

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

[**Reference 8**](#_1ksv4uv)

[**Related Documents 8**](#_a2bhg29tumfn)

# 

# 

# Purpose

The purpose of this policy is to ensure that critical data and systems are backed up on a regular basis, and that the backup copies are stored securely and can be easily restored in the event of a data loss or system failure.

# Scope

This policy applies to all <Company> employees, contractors, third parties who access internal information and business processes.

# Responsibilities

ISMS Manager:

1. The Information Security Manager is responsible for developing and maintaining the backup policy, ensuring compliance with the policy, and conducting regular reviews of the policy.

Backup Administrator:

1. The Backup Administrator is responsible for ensuring that backup operations are carried out in accordance with the backup policy, monitoring backup operations and maintaining backup logs.

Asset Owners:

1. System Owners are responsible for identifying critical and sensitive data and ensuring that it is backed up regularly.

# Policy

## Information backup

1. The backup must be done of selected critical assets in the first place. All company key systems must be backed up as a complete system with imaging processes to enable the quick recovery of the entire system.
2. The company must back up the data in case of data changes, so a continuous backup approach is the best.
3. The backups must be stored with retention copies, at least 3 copies.
4. The considerations must be in place to define the importance of having backups of backups. So, there will be a redundancy to ensure that another can take its place if one backup fails.
5. Backups will be stored both on-site and off-site.
6. Any vendors providing offsite backup storage must be cleared to handle the highest level of information stored.
7. Backups must have at a minimum the following identifying criteria that labels can readily identify:
   * System name;
   * Creation Date;

## Timing

1. The information’s importance must determine the frequency and extent of backups and the acceptable risk determined by the data owner.
2. The backups should be taken on a regular basis for some systems or before and after system updates in case these updates are done rarely. Frequency of taking backups already defined within critical assets.

## Testing

1. Backups’ integrity is periodically tested by performing a data restoration process to ensure that the backup is appropriately working at least yearly. The IT team selects and evaluates a random sample of system backups by restoring it in the test environment. The fixed systems are then verified to ensure that the backup data is functional.
2. Backup verification should be performed regularly.

## Storage

1. Backup copies of operating systems and other critical information system software shall not be stored in the exact location as the operational software.
2. The access to backups is controlled and prohibited from unauthorized access. The cryptography controls must be in place to ensure the security of backup storage.
3. Backup should be compressed to minimize storage requirements

## Retention period

1. The retention period for backups must be determined based on business needs and regulatory requirements.

# 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.12.3.1 Information Backup

# Related Documents

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