**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>**

**Human Resource 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**](#_1t3h5sf)

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

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

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

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

[Policy Statements 6](#_35nkun2)

[Screening 6](#_1ksv4uv)

[Terms and Conditions of Employment 7](#_44sinio)

[Management Responsibilities 7](#_2jxsxqh)

[Information Security Awareness, Education, and Training 7](#_z337ya)

[Disciplinary Process 8](#_3j2qqm3)

[Termination or Change of Employment Responsibilities 8](#_1y810tw)

[The list of responsibilities in the HR processes 8](#_4i7ojhp)

[**Disciplinary actions 9**](#_2xcytpi)

[**Change, Review, and Update 9**](#_1ci93xb)

[**Responsibility 9**](#_3whwml4)

[**Reference 9**](#_2bn6wsx)

[**Related documents 9**](#_qsh70q)

# 

# Purpose

The primary purpose of the Human Resource Security Policy is to ensure that <Company> employees and contractors understand their responsibilities and are suitable for the roles for which they are considered, ensure that <Company> employees and contracts are aware of and fulfill their information security responsibilities, and protect other <Company> interests as part of the process of changing or terminating employment.

# Scope

The policy statements apply to all <Company> resources at all levels of sensitivity, including:

* All full-time, part-time, and temporary staff.
* Contractors, sub-contractors, and consultants are working for or on behalf of <Company>.
* All other individuals and groups who have been granted access to <Company> IT systems and information.

This policy covers all information assets defined in <Company> Risk Assessment and will be a foundation for information security management.

# Policy

This policy will help ensure the safety of the public and a safe working environment at <Company>.

## Policy Statements

### Screening

As <Company> is a company that provides cybersecurity consulting services, the candidates should be chosen carefully. ISMS Manager with HR Generalist must establish formal hiring, resigning, and termination of all <Company> employees.

The HR Generalist must carry out appropriate background verification checks for all candidates for employment, contractor status, or third-party user status:

* Proof of a person’s identity (e.g., passport details).
* Proof of work experience (e.g., resume/CV and references).
* Social networks verification.
* Criminal record checks (optional).

### Terms and Conditions of Employment

1. At the beginning of work, the employee’s legal responsibilities and rights relevant to employment at <Company> must be communicated. They shall be clearly stated in the signed agreement.
2. All <Company> employees must sign an appropriate Non-Disclosure Agreement (NDA) at the time of joining. This agreement shall require the employee to keep the data they receive strictly confidential and comply with applicable <Company> information security policies and procedures.
3. Employees sign NCA (Non-competition agreement).
4. The terms and conditions of employment must include all responsibilities of the users towards information security.

### Management Responsibilities

1. Managers must require all employees, who work under their area of concern, to apply security by <Company> information security policies and procedures.
2. The Management must ensure that employees are:
   1. Appropriately brief on their information security roles and responsibilities.
   2. Encouraged to fulfill <Company’s> information security policies.
   3. Continue to have the appropriate skills and qualifications.
   4. Regularly educated.
3. Managers must be aware of the personal circumstances of their employment; and must be on the lookout for any behavioral change that may lead to security breach or violation.
4. Employees’ paid time off must not affect the availability and performance of service provision at <Company>. Refer to <Company> Employee Handbook, which is stored on our <Company internal resource> page, for further information.

### Information Security Awareness, Education, and Training

1. Suitable information security awareness, training, and education must be provided to <Company> employees, clarifying their responsibilities relating to <Company> information security policies and procedures.
2. ISMS Manager is responsible for:
   1. Preparing an annual information security awareness program and training plan.
   2. Issuing awareness material to keep all <Company> employees aware of their information security roles and responsibilities.
3. Management must allocate sufficient on-the-job time for <Company’s> employees to familiarize themselves with <Company> information security policies, procedures, and the appropriate ways of conducting business.
4. Every <Company> newcomer must pass the Information Security Awareness session and have an interview with HR to check the knowledge of ISMS policies. It must be done within the first week of the hiring date.

### Disciplinary Process

1. The disciplinary process must provide a gradual response taking into consideration factors.
2. Formal disciplinary actions must be taken based on the <Company> Disciplinary Procedure.

### Termination or Change of Employment Responsibilities

1. Responsibilities and practices for performing employment termination or change of employment must be clearly defined and assigned. All actions should occur according to the <Company> Termination Procedure.
2. HR, with the Project Manager, must inform an employee about job duty changes and perform all necessary access rights (logical and physical) to assets.

## The list of responsibilities in the HR processes

| **Role** | **Responsibilities** |
| --- | --- |
| <Name>  Head of HR <Contacts> | * Onboarding * Offboarding * Candidate screening * Exit interview * Outcomes * 1:1 checkpoints * PA * Employee Satisfaction * HR analytics * Budgeting * Market analysis * Events organization control * Official communication on chats * HR policies & procedures * HR team management * ISMS HR documentation reviewing |
| <Name>  CEO  <Contacts> | * Hiring interviews * Terminating process |
| <Name>  Head of Delivery  <Contacts> | * Hiring interviews * Disciplinary process performing |
| <Name>  Project Managers and  Team Leads  <Contacts> | * Hiring interviews for the team * Disciplinary process performing * Initial onboarding into the team * Removing access to all <Company> systems |
| <Name>  Recruiters  <Contacts> | * Clear job descriptions * Searching candidates * Candidate screening * Hiring interviews |
| <Name>  ISMS Manager  <Contacts> | * Security awareness training * HR documentation preparing and updating |

# 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.7.1.1 Screening
* ISO 27001 Annex A.7.1.2 Terms & Conditions of Employment
* ISO 27001 Annex A.7.2.1 Management responsibilities
* ISO 27001 Annex A.7.2.2 Information Security Awareness, Education & Training
* ISO 27001 Annex A.7.2.3 Disciplinary Process
* ISO 27001 Annex A.7.3.1 Termination or change of employment responsibilities

# Related documents

* <Company> Risk Assessment
* <Company> Background Check Procedure
* <Company> Disciplinary Procedure
* <Company> Termination Procedure

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