**ISMS 27001:2022 Getting Started**

|  |  |
| --- | --- |
| Code: | UP-51-0001 |
| Version: | 1.0 |
| Date: | 28.03.2025 |
| Created by: | Ertan Iliyaz |
| Aprroved by: | N/A |
| Confidentiality level: | Public Use |

Evidence

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **By** | **Description** |
| 25.03.2025 | 1.0 | Ertan Iliyaz | A document created and those details provide a simple way to getting started on ISMS. This document is in no way meant as legal or compliance advice. Users of the template must determine what information is necessary and needed to accomplish their objectives. |

Contents

[ISO 27001:2022-Compliant Cybersecurity: Getting Started 3](#_Toc194061247)

[How to demonstrate compliance with Clauses 4.1 and 4.2 5](#_Toc194061248)

[How to demonstrate compliance with Clauses 4.3 and 4.4 5](#_Toc194061249)

[Example roles and responsibilities matrix 6](#_Toc194061250)

[Statement of Management Commitment 7](#_Toc194061251)

[How to demonstrate compliance with Clause 5.1 8](#_Toc194061252)

[How to demonstrate compliance with Clause 5.2 8](#_Toc194061253)

[How to demonstrate compliance with Clause 5.3 9](#_Toc194061254)

[How to demonstrate compliance with Clause 6.1.2 9](#_Toc194061255)

[How to demonstrate compliance with Clause 6.1.3 10](#_Toc194061256)

[How to demonstrate compliance with Clause 6.2 10](#_Toc194061257)

[How to demonstrate compliance with Clause 7.4 10](#_Toc194061258)

[How to demonstrate compliance with Clause 7.5 10](#_Toc194061259)

[How to demonstrate compliance with Clause 8.1 - 8.3 11](#_Toc194061260)

[How to demonstrate compliance with Clauses 7.1-7.3 11](#_Toc194061261)

[Mandatory and non-mandatory documents and records for ISO 27001 12](#_Toc194061262)

[How to demonstrate compliance with Clause 9.1 14](#_Toc194061263)

[How to demonstrate compliance with Clause 9.2 14](#_Toc194061264)

[How to demonstrate compliance with Clause 9.3 14](#_Toc194061265)

[How to demonstrate compliance with Clause 10 14](#_Toc194061266)

[Instructions 16](#_Toc194061267)

[ISO 27001 Documents 17](#_Toc194061268)

[Mandatory Documents and Records 17](#_Toc194061269)

[Non-Mandatory but Expected Documents 19](#_Toc194061270)

[Clauses of ISO 27001:2022 22](#_Toc194061271)

[Statement of Applicability Review (Selected / Grouped Controls) 27](#_Toc194061272)

[People Controls 28](#_Toc194061273)

[Physical Controls 29](#_Toc194061274)

[Technological Controls 29](#_Toc194061275)

# ISO 27001:2022-Compliant Cybersecurity: Getting Started

ISO 27001 Compliance Plan Outline

**Stage 1: Assemble team and develop implementation plan**

• Pull together the people who will be primarily responsible for planning and

implementing ISO 27001 compliance

* Could include:

Project manager

Executive sponsor

Members of security, legal, HR, IT, finance, etc. teams

• Outline the ISO 27001 compliance implementation plan

* + Define information security objectives
	+ Define ISMS goals

• Communicate and raise awareness with your organization about the project

**Stage 2: Scope and baseline ISMS**

• Define the scope of your ISMS

• Conduct a gap analysis to baseline where your organization is today against the ISO requirements

* + Prioritize gaps based on level of effort, impact, and cost
	+ This will give you a road map of next steps and identify spin-off projects

**Stage 3: Implement the ISMS**

• Follow the implementation plan built in stage 1

• Implement any missing requirements identified during the gap analysis in stage 2

in order of priority

• Create a steering committee

• Write information security policies, and get them approved by the steering committee

**Stage 4: Define and implement risk management process**

• Define how your organization identifies, prioritizes, and remediates risks

• Build the risk treatment plan

• Build the risk register

• Begin listing risks found during the previous stages

**Stage 5: Measure, monitor, and review ISMS**

* Implement systems and tools necessary to measure and monitor the ISMS
	+ Could you include security metrics dashboards, regular security review processes, log monitoring systems, third-party reviews of your ISMS, etc.

Use the results of these reviews to continuously improve the state of your ISMS

# How to demonstrate compliance with Clauses 4.1 and 4.2

**Demonstrate compliance with clause 4.1:**

* Work with the subject matter experts in your organization to build a list of external issue that could impact your ISMS – the more detailed, the better
* Do the same for internal issues that could impact your ISMS

Demonstrate compliance with clause 4.2:

* Build a list of interested parties, both internal and external, that are relevant to your ISMS
* Then build a list of their requirements that are relevant to your ISMS

# How to demonstrate compliance with Clauses 4.3 and 4.4

**Demonstrate compliance with clause 4.3:**

* Create a “scope of the ISMS” document

**Demonstrate compliance with clause 4.4:**

* Comply with the rest of ISO 27001

# Example roles and responsibilities matrix

Example Roles and Responsibilities Matrix

|  |  |
| --- | --- |
| **Role**  | **Responsibilities** |
| CEO  | * Provides overall direction, guidance, leadership, and support for the entire organization
* Commits to implementing an information security management system (ISMS) and providing the necessary support
 |
| CIO | * Provides overall direction, guidance, leadership, and

support for the entire information system environment* Assists applicable personnel in their day-to-day operations
* Reports to other members of senior management on a regular basis regarding aspects of the information system posture
 |
| CISO | * Develops, implements, and maintains the information security program
* Ensures the ISMS complies with ISO 27001
 |
| Network engineer System Administration | * Plans, designs, implements, documents, operates, maintains, and optimizes the organization’s network infrastructure
* Manages the organization’s network infrastructure and collaborates with other systems engineers to maintain and optimize the network
 |
| End User | * + Adheres to the organization’s information security policies, procedures, and practices
	+ Reports on instances of noncompliance to senior authorities
	+ Undertakes day-to-day operations while also observing and reporting any issues that could impede the safety
 |
| VendorContractorThird party | * Adheres to the organization’s information security policies, procedures, and practices
 |

# Statement of Management Commitment

**Statement of Management Commitment**

As we are entrusted with critical client information as well as sensitive company assets, the

Board of Directors and Executive Management Team at *[Organization Name]* feel strongly that

our reputation and success depend on safeguarding our own and our *[Customers’/Clients’/*

*Partners’]* information.

Unauthorized disclosure of confidential information could have severe consequences for our

organization, jeopardizing its future and exposing us to legal risks. Similarly, any harm to the

data we rely on for business decision-making and production processes or any delays in

accessing critical information would be unacceptable.

We affirm our intention to treat information security as an integral part of our culture. We show

our commitment to strong security in the following ways:

* + By establishing a Corporate Security Steering Committee and a [Security [Manager/ Security Director/CISO] position within the corporate governance structure
	+ By establishing and communicating clear security policies, standards, and processes
	+ By serving as models of compliance with security policies
	+ By swiftly detecting and dealing with violations of security policies
	+ By allocating sufficient material and human resources to information security
	+ By regularly reviewing and continuously improving our information security program

**Signed and dated**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Organization Leader’s Signature]

# How to demonstrate compliance with Clause 5.1

**Demonstrate compliance with clause 5.1**

* + Write a statement of management commitment to information security, and get it signed by the leader of your organization
	+ Write information about security policy and security objectives that align with the strategic direction of your organization
	+ Show evidence that the ISMS requirements are integrated into your organization’s processes
	+ Provide evidence that the technical and human resources necessary to implement and maintain the ISMS are available
	+ Give evidence of communications with the organization about the importance of the ISMS and following ISMS requirements
	+ Show evidence of monitoring or metrics related to the ISMS that prove it is achieving its intended outcomes
	+ Provide evidence that the people who are responsible for implementing the ISMS are being directed and supported
	+ Show ways that continual improvement of the ISMS has been promoted within the organization
	+ Capture examples of how relevant management roles are supported to contribute to the effectiveness of the ISMS

How to demonstrate compliance with Clause 5.2

**Demonstrate compliance with clause 5.2**:

* Write an information security policy for your organization that meets the requirements of this clause
* Show that it was communicated and is available within your organization
* Show that it was made available to interested parties

How to demonstrate compliance with Clause 5.3

**Demonstrate compliance with clause 5.3:**

* Build a roles and responsibilities matrix
* Show that responsibility and authority for ISO 27001 compliance and reporting have

been assigned to an individual or group

* Communicate organizational roles, responsibilities, and authorities for implementing

and maintaining the ISMS

# How to demonstrate compliance with Clause 6.1.2

**Demonstrate compliance with clause 6.1.2:**

* Document risk assessment process and methodology (mandatory document)
* Build a risk register
* Begin adding known risks to the risk register

# How to demonstrate compliance with Clause 6.1.3

**Demonstrate compliance with clause 6.1.3:**

* + Document your risk treatment methodology
	+ Build a risk treatment plan
	+ Write a statement of applicability
	+ Begin assessing and treating risks

# How to demonstrate compliance with Clause 6.2

**Demonstrate compliance with clause 6.2:**

* + Identify and document the information security objectives for your ISMS
	+ Build a plan to achieve the objectives

# How to demonstrate compliance with Clause 7.4

**Demonstrate compliance with clause 7.4:**

• Document list of communications related to your ISMS, including:

* + When the communications occur
	+ Who receives the communications
	+ Who is doing the communications
	+ How they do them

# How to demonstrate compliance with Clause 7.5

**Demonstrate compliance with clause 7.5:**

* + Ensure that all mandatory documents required by ISO 27001 have been completed
	+ Develop written procedures for document control
	+ Develop written controls for managing records
	+ Develop a written data retention and disposal standard
	+ Ensure that all these procedures and controls are implemented

# How to demonstrate compliance with Clause 8.1 - 8.3

**Demonstrate compliance with clauses 8.1–8.3:**

* + Document the processes that are executed to meet the information security
* requirements of your ISMS
	+ Implement a change management process, and document how it controls
* changes, reviews the consequences of unintended changes, and mitigates any
* adverse effects of changes
	+ Document how your organization determines and controls outsourced processes
* related to its ISMS
	+ Conduct information security risk assessments in accordance with your risk
* assessment methodology on a regular basis
	+ Document the results of information security risk assessments
	+ Implement your information security risk treatment plan
	+ Document the results of information security risk treatment

# How to demonstrate compliance with Clauses 7.1-7.3

**Demonstrate compliance with clauses 7.1–7.3:**

• Provide the right resources to support your ISMS

• Take steps to raise the competence of personnel supporting the ISMS

• Keep records of their competence levels

• Implement a security awareness program that complies with clause 7.3

# Mandatory and non-mandatory documents and records for ISO 27001

**Mandatory documents and records required by ISO/IEC 27001:2022**

* + Scope of the ISMS (clause 4.3)
	+ Information security policy and objectives (clauses 5.2 and 6.2)
	+ Risk assessment and risk treatment methodology (clauses 6.1.2 and 6.1.3)
	+ Statement of Applicability (clause 6.1.3 d)
	+ Risk treatment plan (clauses 6.1.3 e)
	+ Definition of security roles and responsibilities (control 6.2 and 6.6)
	+ Risk assessment report (clause 8.2)
	+ Inventory of assets (control 5.9)
	+ Acceptable use of assets (control 5.10)
	+ Incident response procedure (control 5.26)
	+ Statutory, regulatory, and contractual requirements (control 5.31)
	+ Security operating procedures for IT management (control 5.37)
	+ Definition of security configurations (control 8.9)
	+ Secure system engineering principles (control 8.27)

**Mandatory records:**

* + Records of training, skills, experience, and qualifications (clause 7.2)
	+ Monitoring and measurement results (clause 9.1)
	+ Internal audit program (clause 9.2)
	+ Results of internal audits (clause 9.2)
	+ Results of the management review (clause 9.3)
	+ Results of corrective actions (clause 10.2)
	+ Logs of user activities, exceptions, and security events (control 8.15)

**Non-mandatory documents**

There are many non-mandatory documents that can be used to implement ISO 27001, especially for the security controls from Annex A. These documents are most commonly used:

* + Statement of Management Commitment to Security (clause 5.1)
	+ Procedure for document and record control (clause 7.5 and control 5.33)
	+ Procedure for internal audit (clause 9.2)
	+ Procedure for corrective action (clause 10.2)
	+ Information classification policy (controls 5.10, 5.12, and 5.13)
	+ Information transfer policy (control 5.14)
	+ Access control policy (clause 5.15)
	+ Password policy (controls 5.16, 5.17, and 8.5)
	+ Supplier security policy (controls 5.19, 5.21, 5.22, and 5.23)
	+ Disaster Recovery Plan (controls 5.29, 5.30, and 8.14)
	+ Mobile Device, Teleworking, and Work from Home Policy (controls 6.7, 7.8, 7.9, and 8.1)
	+ Procedures for working in secure areas (controls 7.4 and 7.6)
	+ Clear desk and clear screen policy (control 7.7)
	+ Bring Your Own Device (BYOD) Policy (controls 7.8 and 8.1)
	+ Disposal and destruction policy (controls 7.10, 7.14, and 8.10)
	+ Backup policy (control 8.13)
	+ Encryption Policy (control 8.24)
	+ Change management policy (control 8.32)

# How to demonstrate compliance with Clause 9.1

**Demonstrate compliance with clause 9.1:**

* + Document how your organization monitors, measures, analyzes, and evaluates

security controls related to its ISMS

* + Document how your organization uses the results of its analysis to improve the

effectiveness of its ISMS

# How to demonstrate compliance with Clause 9.2

**Demonstrate compliance with clause 9.2:**

* + Establish and implement an audit program
	+ Select auditors who are impartial and objective
	+ Conduct internal audits on a regular basis, such as annually
	+ Document your internal audit program and how it complies with ISO 27001
	+ Create written audit reports based on the findings of the internal audits
	+ Deliver the audit reports to relevant management
	+ Correct any nonconformities with ISO 27001 found during the internal audits
	+ Retain the audit reports as evidence of your internal audit activity

# How to demonstrate compliance with Clause 9.3

**Demonstrate compliance with clause 9.3:**

* + Schedule and conduct regular management reviews of the ISMS in accordance with the requirements of this clause
	+ Create documented evidence that the management reviews were conducted, including the results of the reviews

How to demonstrate compliance with Clause 10

**Demonstrate compliance with clause 10:**

* + Define and implement a method for addressing nonconformities
	+ Document any found nonconformities
	+ Document corrective actions taken to address nonconformities and prevent them

from happening again

* + Take steps to continually improve your organization’s ISMS

Anex 1:

ISO 27001:2022 Compliance Checklist

# Instructions

This checklist is designed to help organizations assess their compliance with **ISO/IEC 27001:2022** by ensuring that all required documents, controls, and processes are in place. It is divided into the following sections:

1. **Mandatory Documents & Records** – Documents explicitly required for certification.
2. **Non-Mandatory but Expected Documents** – Commonly reviewed during audits to demonstrate best practices.
3. **Clause-Based Compliance Checklist** – Verifies alignment with the core requirements of ISO 27001:2022.
4. **Statement of Applicability Review** – Ensures selected Annex A controls are implemented effectively.

💡 **Tip:** This checklist should be used **alongside your risk assessment and internal audits** to prepare for external certification audits.

# ISO 27001 Documents

## Mandatory Documents and Records

These are explicitly required by ISO 27001:2022 for compliance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document/Record** | **Clause Reference** | **Description** | **Exists?** | **Notes** |
| Scope of the ISMS | Clause 4.3 | Defines the boundaries and applicability of the information security management system, including interested parties and the context of the organisation. |  |  |
| Information Security Policy | Clause 5.2 | Sets the organisation's approach to information security and provides a framework for setting objectives. |  |  |
| ISMS Roles & Responsibilities | Clause 5.3 | Supports Clause 5.3. ISMS Roles and Responsibilities |  |  |
| Risk Assessment Process and Results | Clause 6.1.2 | Documents the criteria, process, and results of risk assessments. |  |  |
| Risk Treatment Process and Plan | Clause 6.1.3 | Outlines selected risk treatment options and actions. |  |  |
| Statement of Applicability (SoA) | Clause 6.1.3 d) | Lists selected controls, justifications, implementation status, and exclusions with reasons. |  |  |
| ISMS Objectives | Clause 6.2 | The objectives summarise the goals for the forthcoming period and must be documented and communicated |  |  |
| Evidence of Competence | Clause 7.2 | Records of training, etc, demonstrating personnel competency in roles affecting information security. |  |  |
| Evidence of Monitoring and Measurement | Clause 9.1 | Demonstrates how performance and effectiveness of ISMS controls are monitored and evaluated. |  |  |
| Internal Audit Plan and Reports | Clause 9.2 | Contains internal audit processes, schedules, and results. |  |  |
| Management Review Minutes | Clause 9.3 | Records outcomes of management review meetings, including key decisions and actions. |  |  |
| Nonconformity and Corrective Action Logs | Clause 10.2 | Tracks nonconformities, corrective actions taken, and their effectiveness. |  |  |
| Control of Documented Information | Clause 7.5 | Documented Information |  |  |

## Non-Mandatory but Expected Documents

These documents are not explicitly required but are commonly expected during audits for effective ISMS implementation.

|  |  |  |  |
| --- | --- | --- | --- |
| **Document/Record** | **Relevance** | **Exists?** | **Notes** |
| Asset Inventory | Control A.5.9 - Inventory of Information Assets  |  |  |  |
| **Access Control Policy** | Supports **Control A.5.15 (Access Control)** and related controls in Annex A. |  |  |
| **Incident Management Procedures** | Supports **Controls A.5.24 - A.5.27 (Incident Management)**. |  |  |
| **Backup Policy** | Supports **Control A.8.13 (Information Backup)**. |  |  |
| **Cryptographic Key Management Policy** | Relevant for **Control A.8.24 (Use of Cryptography)**. |  |  |
| **Supplier Management** | Supports **Controls A.5.19 - A.5.22 (Supplier Relationships and ICT Supply Chain Security)**. |  |  |
| **Physical Security Policy** | Addresses **Controls in Annex A, Controls A.7.1 – A7.14 (Physical Security Controls).** |  |  |
| **Asset Management Records** | Covers **Controls A.5.9 - A.5.11 (Inventory and Acceptable Use of Information and Other Associated Assets)**. |  |  |
| **Business Continuity Plan (BCP)** | Linked to **Controls A.5.30 - A.5.31 (ICT Readiness for Business Continuity and Legal & Contractual Requirements)**. |  |  |
| **Secure Configuration Guidelines** | Aligns with **Controls A.8.9 - A.8.12 (Secure Configuration, Information Deletion, and Data Leakage Prevention)**. |  |  |
| **Training and Awareness Records** | Supports **Controls A.6.3 (Information Security Awareness, Education, and Training) and A.7.2 (Competence)**. |  |  |
| **Secure Development Guidelines** | Supports **Control A.8.25 (Secure Development Life Cycle)**. |  |  |
| **Communications Plans** | Supports **Controls A.7.3 (Awareness) and A.7.4 (Communication)**. |  |  |
| **Special Interest Groups** | Supports **Control A.5.6 (Contact with Special Interest Groups)**. |  |  |
| **Senior Management Support** | Supports **Control A.5.1 (Leadership and Commitment)**. |  |  |
| **Statutory, Regulatory & Contractual Requirements** | Supports **Control A.5.31 (Legal, Statutory, Regulatory & Contractual Requirements)**. |  |  |
| **Cloud Services Policy** | Supports **Control A.5.23 (Information Security for Use of Cloud Services)**. |  |  |
| **Acceptable Use Policy** | Supports **Control A.5.10 (Acceptable Use of Information and Other Associated Assets)**. |  |  |
| **Data Retention Policy** | Supports **Control A.5.33 (Protection of Records)**. |  |  |
| **HR Policy** | Supports **Controls in Clause 6 (People Controls, including Screening, Awareness, and Responsibilities)**. |  |  |
| **Vulnerability & Patching Policy** | Supports **Control A.8.8 (Management of Technical Vulnerabilities)**. |  |  |
| **Password Policy** | Supports **Control A.5.17 (Authentication Information)**. |  |  |

# Clauses of ISO 27001:2022

The following questions confirm if you have aligned your ISMS with the key clauses within the ISO 27001:2022 standard.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Clause Ref** | **Clause Name** | **Question** | **Status [✔/✘]** | **Notes** |
| **4.1** | Understanding the Organization | Have you identified internal and external issues that affect your ISMS? |  |  |
|  |  | Is this documented and reviewed regularly? |  |  |
| **4.2** | Needs and Expectations of Interested Parties | Have you identified stakeholders and their relevant requirements? |  |  |
|  |  | Are these requirements addressed within your ISMS? |  |  |
| **4.3** | Scope of the ISMS | Have you clearly defined the scope of your ISMS, including interfaces and dependencies? |  |  |
|  |  | Is the scope documented and accessible? |  |  |
| **4.4** | ISMS Framework | Is the ISMS established, implemented, and continually improved? |  |  |
|  |  | Are ISMS processes documented, established and managed? |  |  |
| **5.1** | Leadership and Commitment | Does top management demonstrate support and commitment to the ISMS? |  |  |
|  |  | Are information security objectives aligned with organisational strategy? |  |  |
| **5.2** | Information Security Policy | Is there a policy that defines objectives, commitments, and continual improvement? |  |  |
|  |  | Is it documented, communicated, and available to relevant stakeholders? |  |  |
| **5.3** | Roles and Responsibilities | Are roles and responsibilities for ISMS established and communicated? |  |  |
|  |  | Are key ISMS responsibilities assigned and understood by personnel? |  |  |
| **6.1** | Addressing Risks and Opportunities | Have you ISMS risks and opportunities? |  |  |
| **6.1.2** | Risk Assessment | Is there a formal risk assessment process? |  |  |
|  |  | Have controls been selected, justified, and documented in a Statement of Applicability? |  |  |
| **6.2** | Information Security Objectives | Are measurable security objectives established and aligned with organisational goals? |  |  |
|  |  | Are there plans to achieve these objectives? |  |  |
| **7.1** | Resources | Are sufficient resources available for ISMS operation and improvement? |  |  |
| **7.2** | Competence | Is training provided to ensure personnel competence in ISMS-related tasks? |  |  |
| **7.3** | Awareness | Are employees aware of their role in maintaining ISMS effectiveness? |  |  |
| **7.4** | Communication | Is there a process for internal and external communication about ISMS? |  |  |
| **7.5** | Documented Information | Is documentation created, maintained, and controlled effectively? |  |  |
| **8.1** | Operational Planning and Control | Are processes defined and controlled to meet ISMS requirements? |  |  |
|  |  | Are changes to ISMS processes planned and implemented effectively? |  |  |
| **8.2** | (Operational) Risk Assessment | Are risk treatment plan(s) created? |  |  |
|  |  | Is risk documentation kept up-to-date? |  |  |
| **9.1** | Monitoring and Measurement | Are ISMS processes monitored, measured, and evaluated regularly? |  |  |
| **9.2** | Internal Audit | Is there an audit program to review ISMS effectiveness? |  |  |
|  |  | Are audit results documented and acted upon? |  |  |
| **9.3** | Management Review | Does top management review ISMS performance regularly? |  |  |
|  |  | Are inputs and results from the review documented? |  |  |
| **10.1** | Continual Improvement | Have opportunities for ISMS improvement been identified and implemented? |  |  |
| **10.2** | Nonconformity and Corrective Actions | Are issues identified and addressed effectively through corrective actions? |  |  |

# Statement of Applicability Review (Selected / Grouped Controls)

The following controls are selected from Annex A, “The Statement of Applicability”. These are chosen as a cross-section of the controls required but are not exhaustive.

#### **Organisational Controls**

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Reference** | **Control Name** | **Action/Status** | **Notes** |
| 5.1 | Policies for information security | ☐ Documented and approved |  |
| 5.8 | Information security in project management | ☐ Integrated in project plans |  |
| 5.19-5.22 | Third-Party & Supplier Security | ☐ Supplier security requirements assessed and implemented |  |
| 5.23 | Information security for cloud services | ☐ Vendor assessments conducted |  |
| 5.24-5.27 | Incident management (planning, response, learning) | ☐ Procedures tested annually |  |
| 5.34 | Privacy & Protection of PII | ☐ Personal data is protected in compliance with regulations/legislation |  |

## People Controls

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Reference** | **Control Name** | **Action/Status** | **Notes** |
| 6.1 | Screening | ☐ Background checks completed |  |
| 6.3 | Awareness, education, and training | ☐ Sessions conducted quarterly |  |
| 6.5 | Responsibilities after termination/change | ☐ Access revoked immediately |  |

####

## Physical Controls

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Reference** | **Control Name** | **Action/Status** | **Notes** |
| 7.1 | Physical security perimeters | ☐ Entry monitored and logged |  |
| 7.7 | Clear desk and clear screen | ☐ Enforced consistently |  |
| 7.14 | Secure disposal or re-use of equipment | ☐ Procedures in place |  |

##

## Technological Controls

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Reference** | **Control Name** | **Action/Status** | **Notes** |
| 8.7 | Protection against malware | ☐ Anti-malware updated |  |
| 8.9 | Configuration management | ☐ Baselines established |  |
| 8.20 | Network security | ☐ Firewalls and segmentation |  |
| 8.15 | Logging | ☐ Logs are recorded, reviewed and retained |  |
| 8.16 | Monitoring activities | ☐ Logs are reviewed proactively for anomalies |  |
| 8.29 | Security Testing | ☐ Security tests (e.g. penetration tests) are conducted regularly |  |