<Logo>

<Organization Name>

**<Policy Name>**

|  |  |
| --- | --- |
| **Standard** | ISO/IEC 27001:2022 |
| **Version** | <Version No> |
| **Effective Date** | <Date> |
| **Reviewed Date** | <Date> |
| **Next Review Date** | <Date> |
| **Policy Owner** | <Title><Name>/ <Department> |
| **Approved by** | <Title><Name> |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision History** | | | | |
| **Version** | **Date** | **Prepared By** | **Approved By** | **Changes/Notes** |
| <version No> | <DD/MM/YYYY> | <Name> | <Name> | *Initial Version* |

|  |  |  |
| --- | --- | --- |
| **Distribution List** | | |
| **Recipient Name** | **Department** | **Distribution Date** |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |

**Table of Contents**

[Purpose 1](#_Toc179820327)

[Scope 1](#_Toc179820328)

[Policy Objectives 1](#_Toc179820329)

[Roles and Responsibilities 2](#_Toc179820330)

[Policy Statements 3](#_Toc179820331)

[Compliance and Legal Requirements 4](#_Toc179820332)

[Training and Awareness 4](#_Toc179820333)

[Monitoring and Auditing 4](#_Toc179820334)

[Breach of Policy 5](#_Toc179820335)

[Review and Updates 5](#_Toc179820336)

# Purpose

This policy describes <Organization Name>'s approach to <policy purpose>, guaranteeing adherence to ISO 27001:2022 and safeguarding the confidentiality, availability, and integrity of information assets.

# Scope

This policy applies to all employees, contractors, vendors, and any other third parties accessing <Organization Name>’s information systems. It covers all information assets, whether in digital, physical, or cloud formats.

# Policy Objectives

|  |  |
| --- | --- |
| **Asset Management** | To ensure the security of all information assets managed by <Organization Name>. |
| **Information Security** | To protect sensitive and confidential information from unauthorized access, disclosure, alteration, or destruction. |
| **Compliance** | To comply with applicable legal, regulatory, and contractual obligations. |
| **Awareness** | To establish a culture of information security awareness within the organization. |
| **Risk Management** | To ensure that the ISMS is continually improved to mitigate emerging risks and respond to security incidents. |

# Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Policy Owner | Overall responsibility for implementing, maintaining, and improving the new policy. |
| IT Department | Implement and monitor technical controls. |
| HR Department | Ensure that employees are aware of and comply with the policy. |
| Senior Management | Provide strategic oversight, allocate resources for policy implementation, and ensure integration of the policy into the organization’s business strategy. |
| Ensure organizational commitment to information security by enforcing compliance and promoting a security-focused culture. |
| Regularly review the policy's effectiveness and support continuous improvement efforts. |
| Department Heads | Ensure that policy is followed in their respective areas. |
| Report policy violations to the relevant parties. |
| Employees and Contractors | Responsible for complying with the policy. |
| Report security incidents immediately. |
| Third-Party Vendors | Must comply with [Organization Name]’s policies as outlined in contracts and service-level agreements (SLAs). |
| Legal Department | Ensure compliance with applicable legal and regulatory requirements. |

# Policy Statements

**Access Control**

Access to [Organization Name]’s information systems must be limited to authorized personnel only, as per ISO 27001:2022 Annex A.9.

**Data Classification and Handling**

All information must be classified and handled in accordance with its sensitivity (e.g., public, internal, confidential) to ensure data integrity and confidentiality.

**Incident Management**

All security incidents must be reported and managed according to the Incident Handling Procedure (ISO 27001:2022 Annex A.16).

**Physical and Environmental Security**

Ensure physical protection of data assets through controlled access to facilities as defined in ISO 27001:2022 Annex A.11.

**Risk Assessment**

Conduct regular risk assessments to identify potential vulnerabilities and ensure that necessary controls are implemented (ISO 27001:2022 Annex A.12).

*NOTE: Add statements which are relevant to the created new policy.*

# Compliance and Legal Requirements

This policy is aligned with the requirements of ISO 27001:2022. <Organization Name> also ensures compliance with other relevant legal and regulatory requirements, including but not limited to:

* <Relevant legal requirements or regulations>
* <Any additional compliance frameworks>

# Training and Awareness

All employees must complete security awareness training at least annually to ensure understanding and compliance with this policy. Training records will be maintained by the HR Department.

# Monitoring and Auditing

The implementation and effectiveness of this policy will be monitored through regular audits and assessments conducted by <Department Name>. Any deviations from the policy must be reported to <Department Name> for corrective action.

# Breach of Policy

Any violation of this policy may result in disciplinary action, up to and including termination of employment, as per <Organization Name>’s disciplinary procedures.

*Note: The countermeasures for a breach of policy can be changed based on the policy which was violated.*

# Review and Updates

This policy must be reviewed and updated annually or whenever significant changes occur in the organization’s processes, IT infrastructure, or external legal and regulatory requirements.

***Note: This policy document may be adjusted based on the organizational structure, resources, and any specific compliance needs related to ISO 27001:2022.***