Information Security Policy Template

Document Control Information

- **Document Title:** Information Security Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Information Security Policy establishes [ORGANIZATION NAME]'s approach to managing information security in accordance with ISO 27001:2022 requirements. It provides direction for the protection of information assets and outlines the principles for secure information handling throughout the organization.

1.2 Scope

This policy applies to all information assets owned, controlled, or processed by [ORGANIZATION NAME], including: - All information in electronic or physical form - All information systems and networks - All employees, contractors, consultants, temporary staff, and other workers - All external parties that access [ORGANIZATION NAME]'s information systems

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Protecting the confidentiality, integrity, and availability of all information assets - Complying with applicable legal, regulatory, and contractual requirements - Implementing a risk-based approach to information security - Continuously improving the Information Security Management System (ISMS)

2. Information Security Objectives

[ORGANIZATION NAME] has established the following information security objectives: - Protect sensitive information from unauthorized access, disclosure, modification, or destruction - Ensure business continuity and minimize business damage by preventing and reducing the impact of security incidents - Establish a framework for risk assessment and management - Ensure compliance with relevant legislation, regulations, and contractual obligations - Foster a culture of security awareness throughout the organization - [ADD ADDITIONAL OBJECTIVES SPECIFIC TO YOUR ORGANIZATION]

3. Roles and Responsibilities

3.1 Senior Management

- Demonstrate leadership and commitment to the ISMS
- Approve the Information Security Policy
- Ensure integration of ISMS requirements into business processes
- Ensure resources are available for the ISMS
- Communicate the importance of effective information security management

3.2 Information Security Manager/Officer

- Develop, implement, and maintain the ISMS
- Monitor compliance with the Information Security Policy
- Report on the performance of the ISMS to senior management
- Coordinate information security activities across the organization
- Manage information security incidents

3.3 Department Managers

- Implement information security controls within their areas of responsibility
- Ensure staff awareness of information security requirements
- Report information security incidents and weaknesses
- Support information security assessments and audits

3.4 All Staff

- Comply with the Information Security Policy and related procedures
- Protect information assets under their control
- Report information security incidents and weaknesses
- Complete required information security training

4. Risk Management

[ORGANIZATION NAME] shall: - Establish and maintain a documented risk assessment process - Identify information security risks related to assets, processes, and activities - Analyze and evaluate identified risks - Implement appropriate risk treatment options - Review and update risk assessments regularly

5. Information Security Controls

[ORGANIZATION NAME] shall implement controls in accordance with ISO 27001:2022 Annex A requirements, organized into the following categories:

5.1 Organizational Controls

- Information security policies and procedures
- Information security roles and responsibilities
- Segregation of duties
- Contact with authorities and special interest groups
- Threat intelligence
- Information security in project management
- Asset management
- Access control
- Supplier relationships
- Cloud services security
- Business continuity

5.2 People Controls

- Security in human resources
- Security awareness and training
- Disciplinary process
- Termination responsibilities

5.3 Physical Controls

- Physical security perimeters
- Physical entry controls
- Physical security monitoring
- Equipment security
- Clear desk and clear screen

5.4 Technological Controls

- User access management
- Authentication
- Cryptographic controls
- Secure configuration

- Malware protection
- Backup
- Logging and monitoring
- Configuration management
- Information deletion
- Data masking
- Data leakage prevention
- Vulnerability management
- Secure coding

6. Compliance

6.1 Legal and Regulatory Compliance

[ORGANIZATION NAME] shall comply with all relevant legislation, regulations, and contractual requirements related to information security, including but not limited to: - [LIST APPLICABLE LAWS AND REGULATIONS]

6.2 Policy Compliance

Compliance with this policy is mandatory for all employees, contractors, and third parties who have access to [ORGANIZATION NAME]'s information assets. Non-compliance may result in disciplinary action.

6.3 Monitoring and Measurement

[ORGANIZATION NAME] shall monitor and measure the effectiveness of the ISMS and information security controls through: - Regular internal audits - Management reviews - Security assessments - Performance metrics

7. Review and Improvement

This Information Security Policy shall be reviewed at least annually or when significant changes occur to ensure its continued suitability, adequacy, and effectiveness.

8. Related Documents

- Risk Assessment Methodology
- Statement of Applicability
- Information Classification Policy
- Access Control Policy
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

9. Approval

This Information Security Policy is approved by:

Name: ________________________ Position: ______________________ Date:
_________________________ Signature: _____________________