# Information Security Policy Template

## 1. Purpose

This Information Security Policy establishes the framework for ensuring the confidentiality, integrity, and availability of information assets within [Organization Name]. This policy is aligned with the requirements of ISO/IEC 27001:2022 to protect information from unauthorized access, use, disclosure, disruption, modification, or destruction.

## 2. Scope

This policy applies to all employees, contractors, consultants, temporary staff, and any other individuals or entities accessing [Organization Name] information systems or assets. It also encompasses all physical, electronic, and digital information owned, leased, or otherwise controlled by the organization.

## 3. Information Security Objectives

[Organization Name] commits to achieving the following objectives:  
  
- Protect information assets against unauthorized access and breaches.  
- Ensure compliance with applicable legal, regulatory, and contractual requirements.  
- Promote a culture of security awareness and responsibility among employees.  
- Implement and maintain an Information Security Management System (ISMS) to manage risks effectively.  
- Continuously improve security measures through regular assessments and updates.  
  
The organization will measure these objectives using key performance indicators (KPIs) such as the number of incidents reported, the time taken to resolve incidents, and audit findings.

## 4. Roles and Responsibilities

4.1 Information Security Officer (ISO): The ISO is responsible for overseeing the ISMS, ensuring compliance with the ISO 27001 standard, and leading risk management activities.  
4.2 Management: Ensure sufficient resources are allocated for the implementation and maintenance of the ISMS and actively promote information security.  
4.3 Employees: Adhere to the information security policies and procedures, report security incidents, and participate in required training.  
4.4 Third Parties: Comply with [Organization Name] information security requirements as defined in contracts or agreements.  
4.5 Third-Party Accountability: The organization will designate specific personnel to oversee third-party compliance with the organization's information security standards.

## 5. Risk Management

The organization will implement a risk management process to:  
  
- Identify and assess risks to information assets, including physical, electronic, and environmental risks.  
- Implement controls to mitigate identified risks.  
- Review and update the risk assessment periodically or upon significant changes to the environment.  
- Categorize risks by priority to allocate resources effectively.

## 6. Access Control

Access to information assets will be restricted based on the principle of least privilege and need-to-know. Controls include:  
  
- Unique user identification and authentication.  
- Role-based access control (RBAC).  
- Regular review and audit of access rights to ensure ongoing compliance.

## 7. Asset Management

All information assets will be identified, classified, and managed to ensure appropriate levels of protection. The asset management process includes:  
  
- Maintaining an inventory of assets.  
- Assigning asset ownership.  
- Implementing appropriate handling and disposal measures.

## 8. Incident Management

[Organization Name] will establish an incident management process to:  
  
- Detect, report, and respond to security incidents promptly.  
- Document and analyze incidents to prevent recurrence.  
- Communicate incidents to relevant stakeholders as required.  
- Ensure that incidents are resolved within predefined timelines to minimize impact.

## 9. Compliance

The organization will:  
  
- Ensure compliance with relevant laws, regulations, and contractual obligations.  
- Conduct regular internal audits and reviews to assess ISMS performance.  
- Address non-conformities through corrective actions.

## 10. Awareness and Training

Employees and relevant third parties will receive regular information security training to ensure awareness of security risks and responsibilities.

## 11. Continuous Improvement

The ISMS will be continually improved by:  
  
- Monitoring and measuring security performance.  
- Incorporating feedback from audits, incidents, and risk assessments.  
- Reviewing and updating policies, procedures, and controls as necessary.

## 12. Policy Review

This policy will be reviewed at least annually or upon significant changes to ensure it remains relevant and effective. The Information Security Officer (ISO) will be responsible for overseeing the review process.

## 13. Approval

Approved by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 