# Information Security Policy Template

Status – RELEASED

**Document Control**

| | |
|---|---|
| Document Title | <<Document name>> |
| Version | 1.0 |
| Prepared by | <<Client name>> |
| Reviewed by | <<Client name>> |
| Approved by | <<Client name>> |
| Effective date | DD/MM/YYYY |

# 1. Purpose

The purpose of this Information Security Policy is to establish management direction and support for information security in accordance with business requirements, legal obligations, contractual commitments, and applicable regulatory requirements.

This policy defines the organization’s commitment to protecting the confidentiality, integrity, and availability of information assets and maintaining an effective Information Security Management System (ISMS).

# 2. Scope

This policy applies to:

- All employees, contractors, consultants, interns, and third parties
- All business units, processes, and locations
- All information assets, systems, applications, cloud services, and networks owned or managed by the organization

# 3. Objectives

The organization aims to:

- Protect information assets against unauthorized access, disclosure, alteration, and destruction
- Ensure compliance with applicable laws, regulations, and contractual obligations
- Manage information security risks systematically
- Maintain business continuity and operational resilience
- Promote a culture of security awareness and accountability
- Continuously improve the effectiveness of the ISMS

# 4. Information Security Principles

The organization shall:

- Implement risk-based security controls
- Apply least privilege and need-to-know principles
- Secure systems throughout their lifecycle
- Monitor and respond to information security incidents
- Ensure secure handling of customer, employee, and business data
- Maintain compliance with applicable standards and regulations

# 5. Roles and Responsibilities

## 5.1 Top Management

Top Management shall:

- Demonstrate leadership and commitment toward the ISMS
- Approve information security policies and objectives
- Ensure adequate resources are available

## 5.2 ISMS Manager / Information Security Team

Responsible for:

- Managing and maintaining the ISMS
- Conducting risk assessments
- Monitoring compliance and effectiveness
- Reporting security performance to management

## 5.3 Employees and Users

All personnel shall:

- Comply with information security policies and procedures
- Protect organizational assets and credentials
- Report security incidents or weaknesses promptly

## 5.4 Third Parties

Third parties handling organizational information must comply with contractual security obligations and applicable policies.

# 6. Risk Management

The organization shall:

- Identify and assess information security risks
- Apply appropriate treatment measures
- Maintain an information security risk register
- Review risks periodically and upon significant changes

# 7. Asset Management

Information assets shall be:

- Identified and classified
- Assigned ownership
- Protected according to their classification level
- Properly handled during storage, transmission, and disposal

# 8. Access Control

The organization shall implement controls to:

- Ensure authorized access only
- Enforce strong authentication mechanisms
- Periodically review user access rights
- Remove access upon termination or role change

# 9. Cryptography

Appropriate cryptographic controls shall be implemented to protect sensitive and confidential information during storage and transmission.

# 10. Physical and Environmental Security

Physical assets and facilities shall be protected against unauthorized access, damage, theft, and environmental threats.

# 11. Operations Security

The organization shall:

- Maintain secure operating procedures
- Protect against malware
- Monitor systems and logs
- Manage vulnerabilities and patches
- Perform regular backups

# 12. Supplier Security

Security requirements shall be defined and monitored for suppliers, partners, and outsourced service providers.

# 13. Incident Management

All information security incidents shall be:

- Reported promptly
- Investigated appropriately
- Managed to minimize business impact
- Documented and reviewed for lessons learned

# 14. Business Continuity

Information security shall be integrated into business continuity and disaster recovery planning to ensure resilience during disruptions.

# 15. Compliance

The organization shall comply with:

- Applicable legal and regulatory requirements
- Customer and contractual obligations
- Internal policies and procedures
- Relevant industry standards

# 16. Awareness and Training

Employees and relevant stakeholders shall receive periodic information security awareness and role-based training.

# 17. Monitoring and Review

The organization shall:

- Monitor ISMS performance
- Conduct internal audits
- Perform management reviews
- Continuously improve the ISMS

# 18. Policy Violations

Violations of this policy may result in disciplinary action, contractual penalties, or legal consequences, as applicable.

# 19. Policy Review

This policy shall be reviewed at least annually or upon significant business, regulatory, or technological changes.

## Document control

| | |
|---|---|
| **Document owner** | <<Client name>> |
| **Document author** | <<Client name>> |
| **Approval date** | DD-MM-YYYY |
| **Last update date** | DD-MM-YYYY |
| **Reviewers** | <<Client name>> |

**Revision history**

| Version | Summary | Date |
|---|---|---|
| 1.0 | Initial draft | DD-MM-YYYY |
| | | |