

Information Security  
Policy

Enterprise Standards for Information Security (IE3102)

Perera R.Y IT22552488

**Table of Contents**

1. **Introduction** ......................................................................................................................... (Page 3)  
   1.1 Purpose .......................................................................................................................... (Page 3)  
   1.2 Scope .............................................................................................................................. (Page 3)  
   1.3 Information Security Objectives .................................................................................... (Page 4)  
   1.4 Key Definitions ................................................................................................................ (Page 4)
2. **Governance and Responsibilities** ......................................................................................... (Page 5)  
   2.1 Executive Leadership Commitment ............................................................................... (Page 5)  
   2.2 Roles and Responsibilities .............................................................................................. (Page 6)  
   2.3 Information Security Manager ....................................................................................... (Page 6)  
   2.4 IT Personnel .................................................................................................................... (Page 6)
3. **Information Security Principles** ............................................................................................. (Page 7)  
   3.1 Confidentiality, Integrity, and Availability (CIA) .............................................................. (Page 7)  
   3.2 Data Classification and Handling ..................................................................................... (Page 7)  
   3.3 Risk Management Approach ........................................................................................... (Page 8)
4. **Security Policies Overview** ..................................................................................................... (Page 9)  
   4.1 Access Control Policy ........................................................................................................ (Page 9)  
   4.2 Acceptable Use Policy ..................................................................................................... (Page 10)  
   4.3 Data Protection and Privacy Policy ................................................................................. (Page 10)  
   4.4 Remote Access Policy ...................................................................................................... (Page 11)  
   4.5 Password Management Policy ........................................................................................ (Page 11)
5. **Incident Management and Response** ................................................................................... (Page 12)  
   5.1 Incident Reporting Procedure ......................................................................................... (Page 12)  
   5.2 Business Continuity and Disaster Recovery .................................................................... (Page 13)
6. **Compliance and Legal Requirements** .................................................................................... (Page 14)  
   6.1 Compliance with Legal and Regulatory Requirements ................................................... (Page 14)  
   6.2 ISO 27001 Compliance and Audits .................................................................................. (Page 15)  
   6.3 Review and Update of Policy ........................................................................................... (Page 15)
7. **Security Awareness and Training** .......................................................................................... (Page 16)  
   7.1 Training Programs ........................................................................................................... (Page 16)  
   7.2 Awareness Campaigns ..................................................................................................... (Page 16)
8. **Monitoring and Review** ......................................................................................................... (Page 17)  
   8.1 Performance Monitoring and KPIs .................................................................................. (Page 17)  
   8.2 Internal Audits ................................................................................................................. (Page 17)  
   8.3 Continuous Improvement ............................................................................................... (Page 18)
9. **Conclusion** .............................................................................................................................. (Page 19)

**Appendices**  
Appendix A: Glossary of Terms .......................................................................................................... (Page 20)  
Appendix B: Key Contacts and Escalation Procedures ...................................................................... (Page 21)  
Appendix C: Document Control and Revision History ....................................................................... (Page 22)

**1. Introduction**

**1.1 Purpose**

The purpose of this Information Security Policy is to define the framework for protecting [Organization Name]’s information assets. This policy ensures the confidentiality, integrity, and availability of data, in compliance with legal, regulatory, and business requirements. It establishes the foundation for managing information security risks and sets the direction for security activities.

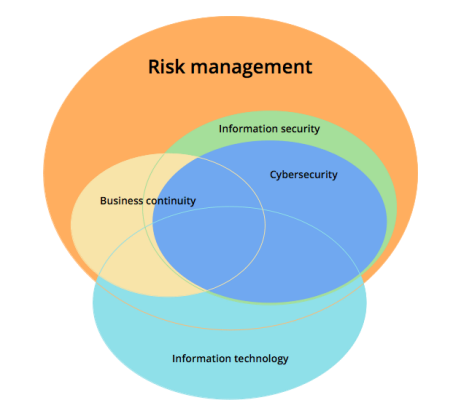
**1.2 Scope**

This policy applies to all employees, contractors, consultants, partners, and any external entities who have access to [Organization Name]’s information systems. It covers all information processing facilities, networks, servers, applications, and data storage, both on-premise and in the cloud.

**1.3 Information Security Objectives**

The objectives of the Information Security Policy are to:

* **Protect Information Assets**: Prevent unauthorized access, disclosure, modification, or destruction of sensitive information.
* **Maintain Operational Continuity**: Ensure that business operations remain functional even during security incidents.
* **Ensure Legal and Regulatory Compliance**: Adhere to applicable regulations such as GDPR, HIPAA, and PCI-DSS.
* **Mitigate Security Risks**: Identify and manage security risks through a structured risk assessment process.
* **Foster a Culture of Security Awareness**: Promote responsible behavior and awareness across the organization.

****

**1.4 Key Definitions**

* **Confidentiality**: Ensuring that sensitive information is accessed only by authorized individuals.
* **Integrity**: Maintaining the accuracy and reliability of data throughout its lifecycle.
* **Availability**: Ensuring that information and resources are accessible when required by authorized users.
* **Information Assets**: Any data, application, hardware, or system that holds value to the organization.

**2. Governance and Responsibilities**

**2.1 Executive Leadership Commitment**

The executive leadership holds ultimate responsibility for the protection of information assets. They provide oversight for the Information Security Management System (ISMS) and ensure it aligns with organizational goals and complies with relevant standards, such as ISO 27001. Leadership ensures sufficient resources, including personnel, budget, and technology, are allocated for the effective implementation of security measures.

**2.2 Roles and Responsibilities**

All employees, contractors, and third-party vendors must adhere to this policy and uphold the principles of information security. The following roles are critical:

* **Executive Leadership**: Responsible for setting security policies and approving the organization’s ISMS framework.
* **Information Security Manager**: Oversees the development, implementation, and maintenance of security programs, ensuring the organization meets ISO 27001 standards.
* **IT Department**: Manages and enforces technical controls, such as firewalls, encryption, and user access management.
* **Department Managers**: Ensure that their teams understand and comply with security requirements.
* **All Employees**: Must follow security protocols and report security incidents or vulnerabilities.

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| **Executive Leadership** | - Approve security policies and the Information Security Management System (ISMS). |
| - Ensure that sufficient resources are allocated for security initiatives. |
| - Set the strategic direction for information security. |
| **Information Security Manager** | - Develop and maintain the ISMS. |
| - Conduct regular risk assessments and manage risk treatment. |
| - Coordinate security incident responses. |
| - Ensure compliance with ISO 27001 and other legal requirements. |
| **IT Department** | - Implement technical controls such as firewalls, encryption, and access control. |
| - Monitor systems for security threats and vulnerabilities. |
| - Ensure secure configurations of networks, systems, and devices. |
| **Department Managers** | - Ensure that teams comply with information security policies and procedures. |
| - Communicate security-related issues and incidents to the Information Security Manager. |
| **Employees/Staff** | - Follow all security policies, including access control and data handling procedures. |
| - Report any suspicious activities or security incidents. |
| - Participate in security awareness training. |
| **Internal Auditor** | - Conduct internal audits of the ISMS to ensure ongoing compliance with ISO 27001 requirements. |
| - Identify and report non-conformities or areas of improvement. |
| **Legal and Compliance Officer** | - Ensure compliance with legal, regulatory, and contractual requirements related to data protection and privacy. |
| **Third-Party Vendors** | - Comply with [Organization Name]’s security requirements when handling sensitive information or accessing systems. |
| - Participate in security risk assessments, where applicable. |

**2.3 Information Security Manager**

The Information Security Manager is the designated person responsible for implementing the ISMS, ensuring that security controls are appropriate and effective. They also ensure that the organization complies with applicable regulations and manages security incidents, audits, and risk assessments.

**2.4 IT Personnel**

IT personnel are responsible for technical control implementation, system monitoring, incident response, and ensuring that systems and infrastructure are secure, patched, and up to date. They manage encryption, network security, and endpoint protection.

**3. Information Security Principles**

**3.1 Confidentiality, Integrity, and Availability (CIA)**

The cornerstone of information security at [Organization Name] is the CIA triad:

* **Confidentiality**: Protect sensitive information from unauthorized access.
* **Integrity**: Ensure that data is reliable, complete, and protected from unauthorized changes.
* **Availability**: Ensure timely access to critical information by authorized users.



**3.2 Data Classification and Handling**

Data classification is essential for determining the appropriate level of protection. [Organization Name] classifies data into the following categories:

* **Confidential**: Information that could cause significant damage to the organization if disclosed. Requires the highest level of security.
* **Internal Use Only**: Non-public information that needs some level of protection but not as strictly as confidential data.
* **Public**: Information that can be shared openly without risk to the organization.

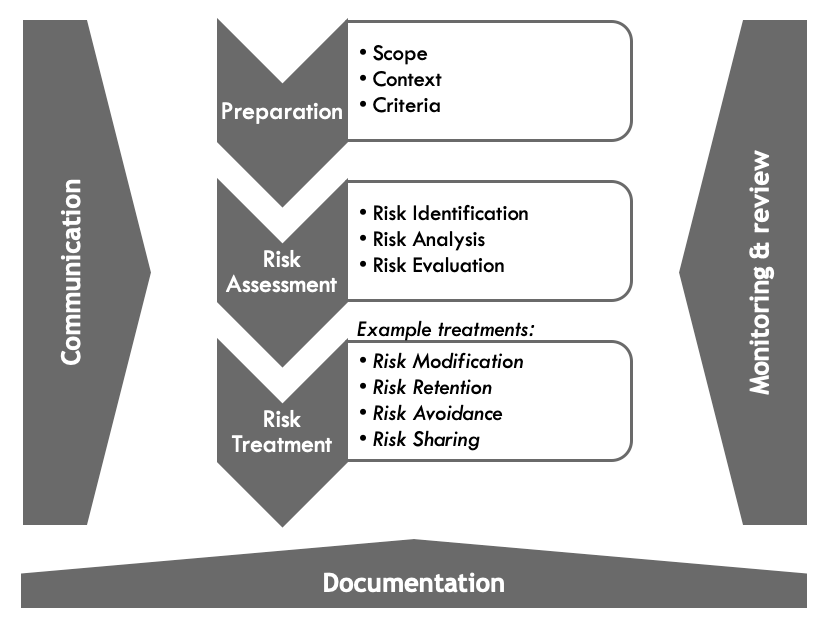
**Handling Requirements**:

* Confidential data must be encrypted both at rest and in transit.
* Access to internal data is restricted to authorized personnel only.
* Public data is not subject to strict control but should be handled responsibly.

**3.3 Risk Management Approach**

[Organization Name] follows a systematic risk management process to identify, assess, and mitigate risks to its information assets. This process includes:

1. **Risk Identification**: Identifying potential security risks that could affect information systems.
2. **Risk Assessment**: Evaluating the likelihood and impact of identified risks.
3. **Risk Treatment**: Implementing measures to mitigate, avoid, transfer, or accept risks based on the organization’s risk appetite.



**4. Security Policies Overview**

**4.1 Access Control Policy**

Access to information systems is granted based on the principle of least privilege. Each employee’s access level is determined by their role, and access is periodically reviewed. Multi-factor authentication (MFA) is required for all critical systems.

**Key Controls**:

* Regular access reviews.
* Immediate removal of access upon employee termination.
* Monitoring of privileged accounts for suspicious activity.

**4.2 Acceptable Use Policy**

Employees are expected to use organizational assets, including computers, mobile devices, and networks, responsibly. Use of corporate systems for personal purposes is limited and must not conflict with security policies.

Examples of acceptable use:

* Accessing the internet for work-related research.
* Sending and receiving work-related email.

**4.3 Data Protection and Privacy Policy**

Personal data, especially that of customers, employees, and third parties, must be handled with care and in compliance with data protection regulations, such as GDPR. Data must be collected only for legitimate business purposes, stored securely, and processed according to privacy laws.

**4.4 Remote Access Policy**

Remote access to [Organization Name] systems is permitted only through secure, encrypted connections such as a Virtual Private Network (VPN). Employees working remotely must follow the same security protocols as those in the office.

**5. Incident Management and Response**

**5.1 Incident Reporting Procedure**

All suspected or actual security incidents must be reported immediately to the Information Security Manager. This includes data breaches, malware infections, and unauthorized access. A formal incident response plan ensures that incidents are addressed promptly, limiting potential damage.

**Key Steps**:

1. **Detection**: Identify the security event.
2. **Reporting**: Notify the Information Security Manager.
3. **Investigation**: Determine the scope and impact.
4. **Mitigation**: Implement corrective actions to contain and resolve the incident.

**5.2 Business Continuity and Disaster Recovery**

In the event of a major incident that disrupts operations, [Organization Name] will invoke its Business Continuity and Disaster Recovery Plans (BCP/DRP) to restore normal operations. Critical systems and data must be backed up regularly, with offsite backups stored securely.

**6. Compliance and Legal Requirements**

**6.1 Compliance with Legal and Regulatory Requirements**

[Organization Name] is committed to adhering to all applicable laws, regulations, and industry standards. This includes data protection laws (e.g., GDPR, CCPA), sector-specific regulations (e.g., PCI-DSS), and international security standards (ISO 27001).

**6.2 ISO 27001 Compliance and Audits**

To maintain compliance with ISO 27001, [Organization Name] will undergo regular internal audits to assess the effectiveness of the ISMS. External audits will also be conducted to ensure that the organization remains certified.

**7. Security Awareness and Training**

**7.1 Training Programs**

All employees, contractors, and third-party users are required to participate in annual security awareness training. This training covers topics such as phishing awareness, safe password practices, and handling sensitive data.

**8. Monitoring and Review**

**8.1 Performance Monitoring and KPIs**

Key Performance Indicators (KPIs) will be established to track the effectiveness of security controls. Regular monitoring and logging of activities will provide insight into whether security measures are achieving their intended outcomes.

**9. Conclusion**

This Information Security Policy is a living document, subject to annual review or updates as necessary. [Organization Name] remains committed to continually improving its security posture to protect its assets and meet regulatory obligations.

**Appendices**

Appendix A: Glossary of Terms  
Appendix B: Key Contacts and Escalation Procedures  
Appendix C: Document Control and Revision History