**Information Security Policy**

Version:

Date:

Classification

Document Control

|  |  |  |
| --- | --- | --- |
| 1. | Document Title: |  |
| 2. | Date of Release: |  |
| 3. | Documents superseded: |  |
| 4. | Version No.: |  |
| 5. | Document Owner: |  |
| 6. | Document Author(s): |  |

Document Approvers

|  |  |  |  |
| --- | --- | --- | --- |
| S. No. | Approver | Approved Through Nominee | Nominee Contact |
|  |  |  |  |

Document Change Approvals

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Section / Page No. | Description of Amendment | Reason for Amendment | New Version No. and Effective Date | Amendment done by | Approved by |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Information Security Policy**

Information security policies form the basis for security principles: protecting the confidentiality, integrity, and availability of available data, and performing data classification to identify information that is important to an organization. Information Security Management System "ISMS" A comprehensive and detailed information security policy document is required, covering all relevant areas of information security and information technology, as guided by ISO 27001.

**Purpose**

The purpose of an information security policy is to select and implement effective and appropriate controls to protect an organization's critical information assets. Her three objectives for information security are: a) Confidentiality b) Integrity c) Availability This policy establishes the basis for information protection, supports security management decisions, and seeks to establish, promote, and ensure those objectives. to. Management of best information security controls and controls.

**Scope**

This policy applies to all physical areas under organizational control. The information security policy should be reviewed regularly by stakeholders to ensure that the policy reflects the changing needs of the organization.

**Objectives**

• Establish direction and commitment to all aspects of information security for the organization.

• Verify that policies are communicated, applied and agreed throughout the organization.

• Ensure that employees comply with established policies.

**Asset Management**

Protecting an organization's information assets requires delegating responsibility and accountability to the right people. To ensure the protection of assets from unauthorized persons.

**Responsibility for Assets**

To identify available assets and documents, an organization can turn to the Asset Register and Asset Inventory. All information assets associated with any type of information system belong to a specific designated entity within an organization. An entity requires a specific person, called the asset owner, to be responsible for the asset.

**Information Classification**

Information can be categorized as follows:

• Internal

• Private.

• Limited.

• Public.

• Confidential

**Human Resources Information Security**

Organizations must ensure that employees are aware of their responsibility to protect information assets and ensure that employees comply with rules and regulations and comply with policies and standards .

**Physical and Environmental Security**

We must ensure that all information assets are protected from physical or environmental threats of any kind. All necessary security controls must be in place to ensure that information assets are not compromised by physical/environmental attacks.

**Work Areas**

• Security perimeters (barriers such as walls, card-controlled entrance gates and doors, and manned reception desks) should be used to protect areas containing information and information systems. • Security perimeters should be clearly defined and all security measures should be implemented.

**Communications and Operations Management**

It is necessary to ensure that all operations of information systems are being carried out properly. The necessary security controls and communication mechanisms should be in place to ensure that day-to-day operations are not compromised in any way.

**Third Party Service Delivery Management**

The organization confirms that the third party does not violate any available standards, laws, regulations, etc. and confirms that the security controls provided by the third party are sufficient to protect the information provided. is needed. When switching third-party services, organizations should closely monitor and manage the transition process and consider the risks involved in procuring third-party services.

**Malicious and Mobile Code Protection**

All necessary detection, preventive, and corrective actions shall be taken to prevent malicious code from affecting information systems. Organizations are responsible for providing staff awareness sessions.

**Backup**

A suitable and effective backup mechanism should be used to ensure that information is not lost in the event of disruption or destruction.

**Network Security Management**

Networks must be protected from all types of cyber-attacks. All necessary security controls should be in place.

**Storage Media Handling**

Removable storage media management procedures shall be established including procedures for the safe disposal of storage media when no longer needed.

**Monitoring**

• Procedures and mechanisms should be used to monitor the use of information resources. We need to track how the system is used.

• Audit logs should be managed effectively. Access Control to Information Systems

• Access control from information systems should be deployed carefully. Required access control should only be granted to those who need it.

• Ensure that the principle of least privilege is followed. Cryptographic Controls

• Required cryptographic protocols should be used to ensure that data cannot be understood by unauthorized persons.

• Use encryption when data is at rest and when data is in transit.

**Information Security Incident Management**

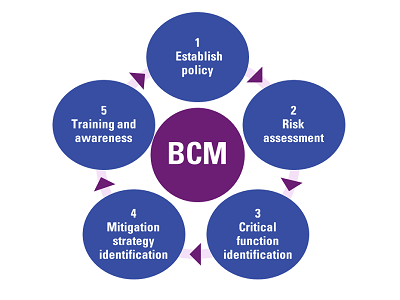
Organizations must follow procedures and mechanisms for identifying, managing, and analyzing security threats and security incidents in real time. All mechanisms should be in place to identify the root causes of incidents, casualties, and damage caused by incidents.Diagram

Description automatically generated

**Reporting Information Security Incidents and Weaknesses**

If an employee discovers or is alerted to a security incident or vulnerability, they should report it to the security department as soon as possible.

**Business Continuity Management**

An organization's critical operations should not be disrupted by random events.

**Roles & Responsibilities**

• The OIMT Director is responsible for information security.

• The OIMT Chief Information Security Officer (CISO) provides technical advisory support to the OIMT Director.