**Information Security Policy**

**Information Security Policy**

The purpose of an information security policy (ISP) is to ensure that all end users and networks within an organization adhere to the bare minimum standards for IT security and data protection. It is designed to make sure that all networks and end users inside a company follow the bare minimum requirements for IT safety and data protection. It is intended to ensure that all internal networks and end users adhere to the strictest standards for data protection and IT security.

**Purpose**

The three goals of Information Security include:

1. Confidentiality
2. Integrity
3. Availability

This Policy sets out the foundation for the protection of information, supporting security management decisions, and directing those objectives to establish, promote, and ensure the best Information Security controls and management of controls.

**Scope**

This Policy applies to all physical areas under the control of the organization. Information Security Policy should be reviewed by respective parties at regular intervals to ensure that the policy is up to date with the organization’s changing requirements.

**Objectives**

* Establish the direction and commitment to all information Security related aspects of the organization.
* Ensure the policy is communicated, applied, and agreed upon throughout the organization.
* Ensure that the employees are complying with the developed policy.

**Asset Management**

To protect the information assets of the organization, the responsibilities and accountabilities should be given to the correct individuals. To make sure that assets are protected from unauthorized individuals.

**Responsibility for Assets**

To identify the available assets and documents, the organization can get the help of an Asset Register and Asset inventory.

All information assets that are associated with any kind of information system, will be owned by a particular designated unit in the organization. In the unit, a designated person should be responsible for the asset, which is known as the asset owner.

**Information Classification**

Information can be categorized in several ways, including;

* Internal
* Private.
* Restricted
* Confidential

**Human Resources Information Security**

To preserve the organization's information assets, it is important to make sure that all employees are aware of their obligations and that they are following all laws, policies, and standards.

**Physical and Environmental Security**

**Work Areas**

* Security perimeters (barriers such as walls, card-controlled entry gates and doors, and manned reception desks) shall be used to protect areas that contain information and information systems.
* Security perimeters shall be clearly defined, and all security measures shall be implemented.
* The protection of all information assets from any physical or environmental threats must be ensured. To ensure that information asset are not harmed by physical or environmental threats, all necessary security procedures should be in place.

**Communications and Operations Management**

The protection of all information assets from any physical or environmental threats must be ensured. To ensure that information asset are not harmed by physical or environmental threats, all necessary security procedures should be in place.

**Third-Party Service Delivery Management**

The organizations must ensure that the third-party businesses adhere to all applicable standards, rules, and regulations, among other things, and must verify that the security controls offered by third parties are adequate to safeguard the information provided to them. The company should carefully monitor and manage the transition process when switching to a third-party provider and should take into account the risks involved in doing so.

**Protection against Malicious and Mobile Code**

To ensure that any kind of malicious code won't impact the information systems, the necessary detective, preventative, and corrective measures should be in place.

The organization is in charge of offering staff awareness training.

**Backup**

To ensure that no information is lost in the case of disruption or destruction, appropriate and efficient backup techniques should be utilized.

**Network Security Management**

The network should be protected from any kind of cyber-attacks. All the required security controls should be in place

**Storage Media Handling**

Procedures shall be established for the management of removable storage media, including procedures for the safe and secure disposal of storage media when no longer required.

**Monitoring**

• Mechanisms and procedures should be employed to keep an eye on how information assets are being used. It is necessary to monitor how the system is used.

•Audit logs ought to be effectively managed.

**Information System Access Control**

* The information systems' access controls should be offered carefully. Only essential individuals should be given access controls.
* Ensure that the concept of least privilege is observed.

**Cryptographic Controls**

* Carefully considered access controls should be provided for the information systems.
* Access controls should only be given to necessary people.
* Make sure the principle of least privilege is upheld.
* Use the necessary encryption techniques to make sure that data cannot be deciphered by unauthorized parties.
* When data is in transit and at rest, use encryption.

**Information Security Incident Management**

To recognize, handle, and analyze security risks or security incidents in real time, an organization must adhere to processes and systems. The systems necessary to identify the incident’s primary cause, its victim, and its damage should be in place.

Diagram

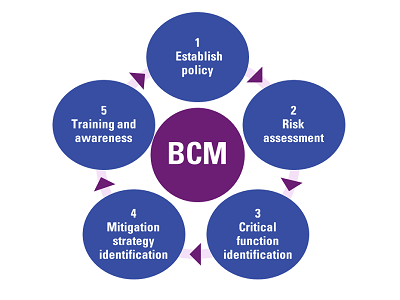
Description automatically generated

**Reporting Information Security Incidents and Weaknesses**

Any security incident or flaw must be reported as soon as feasible by an employee who notices it or receives a warning about it.

**Business Continuity Management**

It is necessary to make sure that unintentional events don't stop the organization's crucial operations



**Roles & Responsibilities**

* The Director, of OIMT is responsible for Information Security.
* The Chief Information Security Officer (CISO), of OIMT provides technical advisory support to the Director of OIMT.