**Acceptable Use 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 | Documents superseded: |  |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 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Acceptable Use Policy**

Information security policies provide the basis for protecting data by providing effective guidelines for acceptable asset use. Information Security Management System "ISMS" Based on ISO 27001, a comprehensive and detailed Acceptable Use Document is required covering all relevant areas of access control and rights

**Purpose**

The primary purpose of the policy is to clearly establish acceptable uses of assets, including all systems and assets that contribute to the essential functions of the organization. This includes PCs, networks, servers, and any kind of asset that can store and process data. The purpose of the policy is to protect employees and the organization. Organizations and employees are exposed to many types of risks when assets are not properly accessed and managed.

**Scope**

This policy applies to all employees, internal and external entities, suppliers, and contractors.

**Usage of Computers:**

• Employees and users should ensure that data stored and processed on computers is backed up daily.

• Users should log off their computers when they are not using, working on, or away from their computers.

• Users should carefully use passwords that comply with the organization's password policy.

• When connecting external devices and drives to your computer, be careful of viruses and malware.

• Users should not use computers to download non-work-related materials.

• Users should not perform scanning or interception of any kind unless it is part of their job duties.

**Usage of Software:**

• Users may not copy copyrighted software provided by the organization onto any type of storage device for personal use.

• Users shall not intentionally or unknowingly download or install malicious software on their systems.

**Security:**

• Users should be responsible for private keys and tokens of all kinds.

• Users should notify security entities when they detect unusual activity in their systems or tokens. Your private key has been compromised.

• Users should ensure that their passwords do not fall into unauthorized hands.

**Usage of E-mail:**

• Users must only use Company-provided e-mail addresses for business purposes.

• All types of information sent by email must be in encrypted form.

• Users should ensure that important emails are backed up regularly.

• Users should be careful and cautious when opening emails from untrusted sources.

• Users should not send harmful or harsh language via corporate e-mail domains.

**Usage of Internet:**

• Users should use only organization-provided Internet connections for work-related activities.

• Users should be very careful when downloading files or software of any kind from untrusted sources.

• User shall not access her social media platform through the Company's Internet connection unless instructed to do so.