**Acceptable Use Policy**

**Acceptable Use Policy**

Through the provision of effective permissible use guidelines for the assets, the information security policy serves as the cornerstone for data protection.

The Acceptable Use Policy document, which covers all relevant areas of access restrictions and privileges, is a requirement of the Information Security Management System (ISMS) regulated by ISO 27001

**Purpose**

The policy's primary goal is to define the appropriate use of resources, encompassing all systems and resources that support the essential operations of the company. Personal computers, networks, servers, and any other type of asset that can store and process data are included in this. The policy's protection of the organization's workers is its main objective. The organization and the employees would be exposed to many types of dangers if assets are not effectively accessible and managed.

**Scope**

All workers, internal entities, external entities, suppliers, and contractors are subject to this policy.

**Usage of Computers:**

* Users and employees are responsible for making daily backups of the data processed and stored by computers.
* Whether not in use, when working on the computer, or when stepping away from the computer, users should log off.
* Users should be informed that they must use passwords that adhere to the organization's password policy.
* Users should be cautious while plugging in external disks and devices for their computers to avoid contracting viruses and malware.
* Users should refrain from downloading anything unrelated to work using the computer.
* Users should avoid performing any scans or intercepting unless it is specifically required by their task.

**Usage of Software:**

* Users must not transfer any form of copyrighted software received from the company to any sort of storage device for their individual use.
* Users should not knowingly or unknowingly download or install any malicious software into the computers.

**Security:**

* Users should be in charge of their private keys and tokens of any kind.
* If users notice any strange behavior in the system or if their tokens or private keys are hacked, they must alert the security unit.
* Users should take precautions to prevent their passwords from falling into the hands of unauthorized individuals.

**Usage of E-mail:**

* Any type of information sent over email should be in an encrypted format, and users should only use the company's email for business purposes.
* Users should ensure that crucial emails are routinely backed up.
* Users should exercise caution and awareness when opening emails from unknown senders.
* Users should refrain from sending any offensive or harsh language using the company's email address.

**Usage of the Internet:**

* Users should only use the organization's internet connection for tasks linked to their jobs.
* When downloading files or any form of software from unreliable sites, users should be alert and cautious.
* Unless specifically instructed, users should avoid utilizing any social networking sites via the company's internet connection.