Cyber Security Guidelines for Employees to follow in the Organization.

# Purpose

The Guideline provides steps to use and protect IT Assets in the organisation to ensure Confidentiality, Integrity, and Availability of the Assets and to prevent any disruptions in operations.

# Scope

This guideline applies to all the Employees who use these assets within the organisation.

# Procedures

## General Awareness

* Understand Cybersecurity Basics:
  + Familiarize yourself with basic cybersecurity concepts like phishing, malware, and ransomware.
* Be Alert and Vigilant:
  + Question unexpected emails, links, or attachments, especially from unknown sources.
  + Report any suspicious activity to the IT or security team immediately.

## Password Management

* Use Strong Passwords:
  + Create complex passwords with at least 12 characters, mixing letters, numbers, and special characters.
  + Avoid using common words, personal information, or sequential patterns.
* Enable Multi-Factor Authentication (MFA):
  + Use MFA for all accounts where it’s available, combining something you know (password) with something you have (device or token).
* Avoid Password Reuse:
  + Never reuse passwords across multiple accounts, especially between work and personal accounts.
* Use Password Managers:
  + Utilize password management tools if possible to securely store and manage passwords.

## Device Security

* Secure Your Devices:
  + Lock your device when unattended, even for a few minutes.
  + Use strong device passcodes.
* Install Updates and Patches:
  + Regularly update operating systems, software, and applications to patch vulnerabilities.
* Use Endpoint Protection:
  + Ensure antivirus and endpoint protection software is installed and up-to-date.
* Avoid Public Wi-Fi:
  + Use a VPN when connecting to public or unsecured networks.

## Email and Communication Security

* Beware of Phishing Attempts:
  + Verify the sender’s email address and scrutinize links before clicking.
  + Verify the sender’s email address and scrutinize links before clicking.
* Avoid Unnecessary Attachments:
  + Open only trusted and expected attachments, and scan them with antivirus software.

## Data Security

* Backup Data Regularly:
  + Ensure critical files are backed up securely, both onsite and in the cloud.
* Limit Data Sharing:
  + Share data only with authorized individuals on a need-to-know basis.
* Dispose of Data Securely:
  + Shred paper documents and securely delete digital files no longer needed.

## Access Control

* Use Principle of Least Privilege:
  + Access only the data and systems required for your role.
* Log Out of Accounts:
  + Always log out after using shared systems or accounts.
* Monitor and Revoke Access:
  + Notify IT to revoke access of an employee when he/she changes roles or leaves the organization.

## Safe Internet Practices

* Avoid Suspicious Websites:
  + Do not visit untrusted or unfamiliar websites.
  + Verify website URLs before entering sensitive information.
* Download Only From Trusted Sources:
  + Avoid downloading software or files from unknown or unverified sources.
* Be Cautious with Social Media:
  + Avoid sharing organizational information on personal social media accounts.
  + Avoid using personal social media accounts on organizational devices to prevent potential cybersecurity risks and distractions.

## Incident Response

* Know How to Report Issues:
  + Familiarize yourself with the process to report security incidents or breaches.
* Respond to Security Alerts:
  + Follow instructions from IT or security teams during security incidents.
* Participate in Drills:
  + Engage in regular incident response exercises or simulations.

## Physical Security

* Protect Physical Assets:
  + Ensure laptops, USB drives, and other devices are not left unattended.
* Secure Workspaces:
  + Use clean desk policies to minimize the risk of sensitive information exposure.
* Restrict Physical Access:
  + Do not let unauthorized individuals into secure areas.
  + Do not permit other employees to use your device unless absolutely necessary. When others do use your device, monitor their activity closely. Never leave your device unattended.

## Remote Work Security

* Use Company-Issued Devices:
  + Avoid using personal devices for work unless explicitly authorized.
* Secure Home Networks:
  + Use strong Wi-Fi passwords and change default router credentials.
* Keep Work and Personal Activities Separate:
  + Avoid using work accounts for personal activities or vice versa.

## Cybersecurity Culture

* Encourage a Security-First Mindset:
  + Promote an organizational culture that prioritizes cybersecurity.
* Continuous Learning:
  + Stay updated on the latest cybersecurity threats and best practices.
* Zero Trust Approach:
  + Adopt a “trust but verify” stance toward systems, individuals, and devices.