Information Security Policy

[Organization Name]
Version 1.0

Purpose

The purpose of this policy is to set required procedures for managing, reviewing and validating user access to information, equipment, facilities and systems.

Scope

This policy is applied to all to all systems, equipment, facilities and information used within the ISMS scope. It is also applied to all users of the organization.

Policy Statement

General

Access rights to sensitive data, systems and facilities will be based on the functional roles of staff, contractors, visitors and other users of the [ORGANIZATION] IT infrastructure, applications and data.

Access will be granted based on:

- Least Privilege: Users will only be granted access to PHI for the purpose of executing their responsibilities and duties. Right to access information, systems and facilities shall not be granted unless there is a legitimate business need.
- Segregation of Duties: Users should not be able to grant themselves rights. Administrative accounts shall be monitored. To the maximum extent logs shall be maintained.
- Role Based Access: Users will be assigned access rights to information, system and facilities based on functional roles they assume in the course of doing the [ORGANIZATION] business.

Generic or group IDs shall not normally be permitted as means of access to the company data, but may be granted under exceptional circumstances if sufficient other controls on access are in place.

Access to the company IT resources and services will be given through the provision of a unique user account and complex password.

Physical access across the company campus, where restricted, is controlled primarily via the company access Cards

Account Types

Provisioning of accounts and their privileges across [ORGANIZATION] systems and applications must conform to the following requirements.

- Default Accounts : Default accounts shall be disabled removed or renamed for all devices. Passwords for all renamed default accounts must be changed before activation.
- Service or Process Accounts: Service or Process account settings are defined in the System Configuration Policy and associated procedures.
- Generic Accounts: Disabled generic accounts may be used as templates to create new accounts of various types as long as names and default passwords are changed in conformance with the Password Policy.
- Privileged Accounts: Administrator and other privileged accounts shall be created only where needed to manage the system.
- Individual User Accounts : Each user account will be assigned one or more roles based on the user's access requirements.
- Temporary Accounts: From time to time temporary accounts will need to be created to allow work by short term contractors, guests or auditors.
- External and Contractor Accounts : External users and contractors must meet the same standards as Temporary account holders.

Privilege Management

Privileges access to systems, information and facilities are allocated in the following way:

System/Facility/Network	**Authorized person to grant/remove access rights**	**Method of authorization**
i.e. Accounting System	I.e Finance Manager	Email

Review of Access Rights

Owners of each system and owners of facilities must review the access right at the following intervals :

System/Facility/Network	Time interval for review
I.e Accounting System	Every 6 months

Password Management

- All user-level and system-level passwords must conform to the *Password Construction Guidelines*.
- Users must use a separate, unique password for each of their work related accounts.
- Users may not use any work related passwords for their own, personal accounts.
- Passwords should be changed only when there is reason to believe a password has been compromised.
- Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.
- Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential <Company Name> information.
- Passwords must not be inserted into email messages, nor revealed over the phone to anyone.
- Passwords may be stored only in “password managers” authorized by the organization.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.
- Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

Policy Review

This policy shall be reviewed and updated regularly by the [ROLE] and an auditor external to the company if required to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

[job title]
[name]

_____
[signature]