Access Control Policy

# 1. Purpose

The purpose of this Access Control Policy is to ensure that access to information and information systems is granted only to authorized users, based on the principle of least privilege, to protect the confidentiality, integrity, and availability of organizational assets.

# 2. Scope

This policy applies to all employees, contractors, and third-party users who access the organization's information systems and data.

# 3. Policy

- User access must be approved by management and granted based on job responsibilities.  
- Multi-factor authentication (MFA) shall be implemented for remote and administrative access.  
- Access rights shall be reviewed quarterly and revoked promptly upon termination of employment.  
- Users must not share passwords or use shared accounts.  
- Access to sensitive data must be logged and monitored.

# 4. Responsibilities

The IT department is responsible for implementing and enforcing this policy. Department heads are responsible for approving user access rights.

# 5. Review and Updates

This policy shall be reviewed annually or following significant changes to the organization's IT infrastructure.