SOP: User Access Controls and Authentication Procedures

1. Purpose

This SOP defines the **user access controls and authentication procedures** essential for securing information systems. It includes guidelines on creating and managing user accounts, enforcing password policies, implementing multi-factor authentication, and regularly reviewing access privileges. The purpose is to ensure that only authorized individuals can access sensitive data and systems, thereby protecting organizational assets from unauthorized access and potential security breaches.

2. Scope

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

3. Definitions

Term	Definition
User Account	An identity established for a person or system to grant access to organizational resources.
Authentication	The process of verifying the identity of a user, process, or device.
Multi-Factor Authentication (MFA)	An authentication method requiring two or more verification factors to gain access to a resource.
Privilege Authorization	Granting appropriate access rights based on roles and responsibilities.

4. Responsibilities

- **IT Department:** Manage user access, maintain authentication systems, and conduct regular access reviews.
- **Managers:** Approve access requests and report changes in user roles or employment status.
- **All Users:** Adhere to password policies and report suspected security incidents.

5. Procedures

5.1 User Account Creation

1. All new access requests must be submitted through the official access request form and approved by the user's supervisor or manager.
2. The IT Department creates user accounts based on the principle of least privilege.
3. User identities must be unique; sharing of accounts is prohibited.

5.2 Password Policy

1. Passwords must meet the following requirements:
    - Minimum length of 12 characters
    - Include upper- and lower-case letters, numbers, and special characters
    - Changed every 90 days
    - CANNOT reuse last 5 passwords

2. Default passwords must be changed upon first login.

5.3 Multi-Factor Authentication (MFA)

1. MFA is required for all remote access and privileged accounts.
2. Acceptable second factors include SMS, authenticator apps, or hardware tokens.

5.4 Access Review and Privilege Management

1. Conduct access reviews at least semi-annually to ensure privileges are appropriate.
2. Immediately revoke access for terminated or transferred users.
3. Adjust user permissions upon changes in job roles or responsibilities.

5.5 Account Deactivation

1. Upon employment termination or role change, access must be disabled within 24 hours.
2. Inactive accounts should be reviewed and removed after 60 days of inactivity.

6. Documentation

- Document all user access requests, approvals, changes, and deactivations.
- Maintain an access review log with dates, reviewers, and findings.

7. Enforcement

Non-compliance with this SOP may result in disciplinary action, including suspension of access privileges, additional training, or other actions as deemed necessary by management.

8. Review and Update

This SOP should be reviewed at least annually or after significant changes to information systems or organizational structure. Updates must be approved by IT management.