SOP: User Account Creation and Authentication Procedures

This SOP details the **user account creation and authentication procedures**, including steps for secure account registration, verification processes, password policies, multi-factor authentication implementation, user role assignment, and account activation protocols. The objective is to ensure secure and efficient access management, protect user data, and maintain system integrity through standardized authentication workflows.

1. Purpose

To define a standardized approach for user account creation, verification, secure authentication, password management, user role assignment, and activation, ensuring the confidentiality, integrity, and availability of user data and system resources.

2. Scope

This procedure applies to all users requiring access to the system(s), including employees, contractors, and authorized third parties.

3. Responsibilities

Role	Responsibility
System Administrator	Oversee user account creation, enforce authentication and password policies, assign roles, monitor account activity.
User	Provide accurate information, follow authentication guidelines, maintain security of credentials.
IT Security	Review logs, manage password resets, investigate suspicious activity, audit adherence to SOP.

4. Procedure

4.1 User Account Registration

1. User accesses the registration page via secure (HTTPS) connection.
2. User provides required information (e.g., full name, email address, phone number).
3. System checks for duplicate accounts using unique identifiers (e.g., email).
4. User is informed of privacy policy and must consent to data processing.
5. Registration request is recorded in a secure audit log.

4.2 Verification Process

1. An automated email or SMS is sent to the user containing a unique verification link or code.
2. User must complete verification within a defined time window (e.g., 24 hours).
3. Upon successful verification, account status is updated to "Verified."
4. Unverified registrations are purged after the expiration period.

4.3 Password Policies

- Minimum password length: 12 characters
- Require upper and lower case letters, numbers, and special characters
- Prohibit reuse of last 5 passwords
- Forced password change on initial login
- Passwords stored using strong cryptographic hashing (e.g., bcrypt, Argon2)
- Provide guidance for creating strong passphrases

4.4 Multi-Factor Authentication (MFA)

1. User is prompted to enroll in MFA during first login or after password reset.
2. MFA options offered (e.g., authenticator app, SMS code, hardware token).
3. User must register at least one MFA method before proceeding.
4. MFA is required for all subsequent authentications or sensitive operations.
5. MFA enrollment and changes are logged.

4.5 User Role Assignment

1. During account creation, system assigns default role (e.g., "User").
2. Elevated roles (e.g., "Admin," "Manager") require approval from designated authority.
3. Role assignments are documented and reviewed regularly.
4. Principle of least privilege applies to all role assignments.

4.6 Account Activation Protocol

1. After verification and MFA enrollment, account status is set to "Active."
2. User receives confirmation via email/SMS and may log in.
3. Inactive or unverified accounts are disabled or deleted per retention policy.
4. Account changes (activation, deactivation) are logged.

5. Review and Audit

- Regularly review logs for unauthorized account creations or failed authentication attempts.
- Audit user roles and access levels biannually.
- Update SOP as required to respond to emerging security threats.

6. References

- NIST SP 800-63B Digital Identity Guidelines
- ISO/IEC 27001 Information Security Management
- Company Privacy Policy

Note: Non-compliance with this SOP may result in revocation of system access and disciplinary action in accordance with company policy.