Standard Operating Procedure (SOP)

User Authentication and Verification Process

This SOP describes the **user authentication and verification process**, covering the steps for secure user identity validation, multi-factor authentication methods, password management protocols, account recovery procedures, session management, and security monitoring. The goal is to ensure authorized access, protect user data, and maintain system integrity through reliable verification techniques and compliance with security standards.

1. Scope

This SOP applies to all systems and applications where user authentication and verification are required to access sensitive information or perform critical operations.

2. Responsibilities

- **System Administrators:** Implement and maintain authentication mechanisms.
- **Users:** Follow secure authentication and password management practices.
- **Security Team:** Monitor authentication activities and respond to incidents.

3. User Authentication Procedures

1. **Registration / Onboarding**
    - Collect required user information (e.g., email, phone, identity proof as needed).
    - Send verification (e.g., email confirmation, SMS OTP) to validate contact information.
2. **Login Authentication**
    - Username and password entry.
    - Password input must be protected (masked input, TLS transmission).
    - Hash & salt passwords before storage (do not store plain text passwords).
3. **Multi-Factor Authentication (MFA)**
    - Support MFA methods:
        - Time-based One-Time Password (TOTP), e.g., authenticator app.
        - SMS or email OTP (where stronger methods are not possible).
        - Biometric (if applicable).
    - Prompt MFA after password authentication or as risk/adaptive triggers require.

4. Password Management Protocol

1. Password requirements:
    - Minimum 8 characters (preferably 12+), with upper/lowercase, numbers, and special characters.
    - Disallow common passwords and recent breaches.
2. Enforce password expiration (e.g., every 180 days) if required by regulation.
3. **Password Reset:**
    - Use password reset tokens sent by secure channel (email/SMS/phone verification).

- Expire reset tokens after a short duration (e.g., 30 minutes).

5. Account Recovery Procedures

1. Verify user identity via registered email/phone and, if available, backup codes or security questions.
2. Lock account after repeated failed recovery attempts.
3. Notify user of any account recovery activities via original email/phone.

6. Session Management

- Expire sessions after a period of inactivity (e.g., 15-30 minutes).
- Use secure, HttpOnly, and SameSite cookies for session tokens where applicable.
- Immediately revoke sessions upon password change, logout, or suspicious activity.
- Allow users to view and terminate active sessions/devices.

7. Security Monitoring & Compliance

- Log all authentication and verification events.
- Monitor for suspicious login and access patterns.
- Conduct regular reviews and audits of authentication mechanisms.
- Comply with regulations (e.g., GDPR, HIPAA, PCI-DSS) as applicable.
- Update authentication protocols as new threats and standards emerge.

8. References

- OWASP Authentication Cheat Sheet
- NIST Digital Identity Guidelines (SP 800-63B)
- Company Information Security Policy