SOP: Password Reset and Account Management Procedures

This SOP details the **password reset and account management procedures**, including steps for verifying user identity, secure password creation guidelines, account lockout and recovery processes, user access level adjustments, multi-factor authentication setup, and documentation of account changes. The objective is to maintain account security and provide efficient support for users experiencing login issues or requiring account modifications.

1. Scope

This procedure applies to all users and administrators responsible for managing user accounts and credentials across organizational platforms and systems.

2. Responsibilities

- **Users:** Report issues related to account access promptly and comply with security guidelines.
- **IT Support:** Authenticate identity, process password resets, manage access levels, and document changes.
- **IT Security:** Monitor account activity, perform audits, and enforce policy compliance.

3. Procedure

3.1. User Identity Verification

1. Confirm user's identity using at least two verification methods:
    - Official photo ID (if in person)
    - Verified email or phone callback
    - Security questions unique to the user
    - Supervisor or manager attestation (if applicable)
2. Log verification steps and outcome in the support ticketing system.

3.2. Secure Password Creation Guidelines

- Minimum length of 12 characters
- Must include uppercase and lowercase letters, numbers, and special characters
- Prohibit use of easily guessable words or previous passwords
- Encourage use of passphrases
- Passwords must not be shared or recorded in insecure manners

3.3. Password Reset Process

1. Confirm user identity as per section 3.1.
2. Initiate password reset via authorized admin panel or tool.
3. Communicate reset instructions securely to the user.
4. Require immediate password change upon next login.
5. Close the ticket after user confirms access.

3.4. Account Lockout and Recovery

- Accounts automatically lock after **5** consecutive failed login attempts.
- Users must contact IT Support to request account unlock.
- Follow identity verification (section 3.1) before unlocking.
- Audit unlocked accounts for suspicious activity and report if necessary.

3.5. User Access Level Adjustments

1. Receive documented request for access level changes with managerial approval.
2. Implement changes adhering to the principle of least privilege.
3. Test and confirm updated access with user and supervisor.
4. Record adjustments in the change management log.

3.6. Multi-Factor Authentication (MFA) Setup

1. Guide user through MFA enrollment process (e.g., mobile app, hardware token, SMS code).
2. Verify successful activation and test MFA functionality.
3. Provide user with instructions for recovery options if MFA device is lost.

3.7. Documentation of Account Changes

- Log all account modifications, including timestamps and staff responsible, in the designated system.
- Ensure sufficient detail for audit trails and compliance purposes.
- Regularly review access and activity logs for anomalies.

4. References

- IT Security Policy
- Acceptable Use Policy
- Incident Response SOP

5. Revision History

Date	Revision	Description	Editor
2024-06-12	1.0	Initial release	IT Security Team

For questions or to report incidents, contact the IT Support Desk immediately.