SOP Template: Account Access and Password Reset Procedures

This SOP details the **account access and password reset procedures**, covering user authentication protocols, secure password creation guidelines, step-by-step instructions for resetting forgotten passwords, verification methods to confirm user identity, and measures to prevent unauthorized access. The goal is to maintain account security and ensure users can regain access efficiently while protecting sensitive information.

1. User Authentication Protocols

- All users must authenticate using their unique username and password.
- Multi-factor authentication (MFA) is required for all privileged accounts and recommended for all users.
- Sessions automatically expire after 15 minutes of inactivity.

2. Secure Password Creation Guidelines

- Minimum length: 12 characters
- Include uppercase and lowercase letters, numbers, and special characters.
- No dictionary words or easily guessed patterns (e.g., "Password123").
- Password must not match previous 6 passwords.
- Passwords should be changed every 90 days.

3. Password Reset Procedures

1. User clicks "Forgot Password" on the login page.
2. User enters their registered email address.
3. System sends a password reset link to the registered email.
4. User clicks the link, which redirects to the password reset page.
5. User creates a new password following the secure password guidelines.
6. System confirms the reset and notifies the user via email.

Note: The password reset link expires in 60 minutes for security purposes.

4. User Identity Verification Methods

- Email verification (sending a unique token to the registered email address).
- Security questions (configurable by the user; required only if email is inaccessible).
- SMS verification (if enabled and mobile phone number is on file).
- Manual verification by support staff for high-risk cases (e.g., financial or admin accounts).

5. Measures to Prevent Unauthorized Access

- Lock accounts after 5 failed login attempts for 30 minutes.
- Monitor account activity and notify users of any suspicious login attempts.
- Enforce strong password policies as outlined above.
- Regularly update and patch authentication systems and related software.
- Access to the password reset function is monitored and logged for audit purposes.

6. Roles and Responsibilities

Role	Responsibility
User	Maintain secure passwords, follow reset procedures, report suspicious activity.
IT Support	Assist users with account access issues, perform identity verification, escalate high-risk cases.

System Administrator	Enforce authentication protocols, monitor security logs, update password policies.

7. Related Documentation

- IT Security Policy
- User Account Management Policy
- Incident Response Plan

8. Revision History

Date	Version	Description	Author
2024-06-10	1.0	Initial SOP template creation	AI Assistant