STANDARD OPERATING PROCEDURE

Password Reset SOP

Document no.	SOP-IT-003
Revision	1.0
Owner	IT Security Manager
Effective date	September 15, 2026
Review cycle	Every 6 months

1. Purpose

To verify a requester's identity before any password reset or account unlock, and to restore access securely without exposing the organization to social engineering or unauthorized account takeover.

2. Scope

Applies to self-service and help-desk assisted password resets and account unlocks for employee accounts in the identity provider and connected applications. New account creation and privileged administrator credential resets are covered by other procedures.

Definitions

Identity verification	Confirming a requester is who they claim to be before making any change to their account.
Social engineering	An attempt to manipulate a person into bypassing security controls, such as urgent or impersonation-based reset requests.
MFA re-enrollment	Registering a new device or method for multi-factor authentication after a lost or replaced device.
Account lockout	A security control that disables sign-in after repeated failed login attempts.

3. Responsibilities

Service Desk Analyst	Verifies identity, logs the request and delivers the new credential securely.
System Administrator	Reviews sign-in activity, performs the reset or unlock, and manages MFA re-enrollment.
End User	Requests the reset, completes identity verification and confirms successful login.

RACI matrix

Activity	Service Desk Analyst	System Administrator	End User
Receive and verify the reset request	R/A	I	C
Check sign-in activity for suspicious behavior	C	R/A	I
Reset the password or unlock the account	C	R/A	I

Activity	Service Desk Analyst	System Administrator	End User
Confirm login and close the ticket	R/A	I	C

R = Responsible, A = Accountable, C = Consulted, I = Informed

4. Materials and PPE

Materials, tools and systems

- Identity provider admin console
- Ticketing system
- Identity verification checklist
- MFA management tool
- Password complexity policy reference

5. Procedure

Step	Task	Owner	Done
5.1	**Receive the reset request** The Service Desk Analyst logs a ticket noting the request channel, whether self-service portal, phone or chat, and the stated reason for the reset or unlock.	Service Desk Analyst	☐
5.2	**Verify the requester's identity** The Service Desk Analyst verifies identity using an approved method, such as a callback to the number on file, security questions, or manager confirmation, before touching the account. **Checkpoint:** No account change is made until identity is positively verified, regardless of how urgent the request sounds. **Warning:** Watch for social engineering: urgency, impersonating an executive, or refusing standard verification are all red flags.	Service Desk Analyst	☐
5.3	**Confirm account details match** The Service Desk Analyst confirms the account, department and manager on the request match the identity provider record exactly.	Service Desk Analyst	☐
5.4	**Review sign-in activity** The System Administrator reviews recent sign-in and audit logs for the account to check for suspicious activity or an unusual lockout reason before proceeding. **Checkpoint:** Requests tied to suspicious sign-in activity are escalated to security before any reset is performed.	System Administrator	☐
5.5	**Reset the password or unlock the account** The System Administrator resets the password or unlocks the account in the identity provider, setting the account to require a password change at next login.	System Administrator	☐
5.6	**Confirm password policy is enforced** The System Administrator confirms the identity provider applies the standard password complexity policy to the new temporary password.	System Administrator	☐
5.7	**Handle MFA re-enrollment if needed** If the request involves a lost or replaced device, the System Administrator re-enrolls MFA only after completing an additional layer of verification beyond the standard reset check. **Warning:** MFA re-enrollment is higher risk than a password reset alone and requires stronger verification before proceeding.	System Administrator	☐

Step	Task	Owner	Done
5.8	**Deliver the temporary credential securely** The Service Desk Analyst delivers the temporary password through a channel separate from the one used to make the request, such as a phone call after a portal request.	Service Desk Analyst	☐
5.9	**Confirm successful login** The Service Desk Analyst confirms with the end user that they logged in successfully and completed the required password change. **Checkpoint:** The ticket is not closed until the user confirms they can sign in.	Service Desk Analyst	☐
5.10	**Log the verification method used** The Service Desk Analyst records which verification method was used and any notes on the reason for the reset in the ticket.	Service Desk Analyst	☐
5.11	**Close the ticket** The Service Desk Analyst closes the ticket once login is confirmed and documentation is complete.	Service Desk Analyst	☐

6. Quality checks

- Every reset ticket records which identity verification method was used.
- No password is reset or account unlocked without positive identity verification.
- MFA re-enrollment requests go through the additional verification step before completion.
- Reset requests tied to suspicious sign-in activity are escalated to security before completion.

7. Records

- Password reset ticket with verification method noted
- Sign-in log excerpt for escalated or suspicious cases
- MFA re-enrollment confirmation

8. KPIs

- Average time to complete a verified reset
- Percentage of resets completed through self-service
- Number of resets escalated for suspicious activity

9. Common mistakes

- Resetting a password from an emailed request without verifying the sender out of band.
- Skipping the sign-in activity check before resetting a locked account.
- Sending the username and the new temporary password in the same message.
- Not requiring a password change at the next login after a reset.

10. Revision history

Revision	Date	Description	Reviewed by
1.0	September 15, 2026	Initial release	Ilia Pirozhenko

Approval

Prepared by	Approved by	Date

This is a template. Adapt it to your organization, equipment and local regulations before use.

Scan for the latest version

Opens this template online, where you can download it again in Word, PDF, Excel or CSV — free, no sign-up.

Or add it to Perfect Wiki so your team can find it and ask questions about it in Microsoft Teams, Slack, kChat or Mattermost.