STANDARD OPERATING PROCEDURE

User Account Provisioning SOP

Document no.	SOP-IT-001
Revision	1.0
Owner	IT Service Delivery Manager
Effective date	September 15, 2026
Review cycle	Every 12 months

1. Purpose

To make sure every new hire receives working accounts and only the access their role requires, granted with manager approval and secured with multi-factor authentication before day one.

2. Scope

Applies to creating new employee identities, mailboxes, group memberships and application access requested through HR onboarding. Password resets and periodic access reviews for existing employees are covered by separate SOPs.

Definitions

Onboarding ticket	The ticket raised in the ticketing system to request a new hire's accounts and access.
Identity provider (IdP)	The system of record for user identities, used for single sign-on and account creation.
Least privilege	Granting only the access a role needs to do its job, and no more.
Role-based access profile	A predefined set of application and group access mapped to a job role or department.

3. Responsibilities

Service Desk Analyst	Validates onboarding requests, delivers credentials, and confirms the new hire can log in.
System Administrator	Creates identities, provisions accounts and application access, and configures MFA.
Hiring Manager	Approves the access profile and scope requested for the new hire.
HR Coordinator	Submits the onboarding request with role, department and start date.

RACI matrix

Activity	Service Desk Analyst	System Administrator	Hiring Manager	HR Coordinator
Submit the onboarding request	I	-	C	R/A
Approve the requested access scope	I	-	R/A	C
Create identity and provision accounts	C	R/A	I	-

Activity	Service Desk Analyst	System Administrator	Hiring Manager	HR Coordinator
Verify least-privilege access is applied	R/A	R	I	-
Deliver credentials and confirm login	R/A	C	I	I

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

4. Materials and PPE

Materials, tools and systems

- Onboarding ticket in the ticketing system
- Identity provider admin console
- Role-based access profile template
- MFA enrollment tool
- Access register or asset management system
- Secure credential delivery channel

5. Procedure

Step	Task	Owner	Done
5.1	**Receive the onboarding request** The HR Coordinator submits the onboarding ticket with the new hire's name, start date, job title, department and manager. The ticket must reach the service desk at least two business days before the start date.	HR Coordinator	☐
5.2	**Verify request and approval are complete** The Service Desk Analyst checks that the manager's approval of the requested access scope is attached to the ticket before doing any work. **Checkpoint:** The account is never created until manager approval is attached to the ticket, regardless of the start date.	Service Desk Analyst	☐
5.3	**Select the role-based access profile** The System Administrator matches the new hire's job title and department to the standard role-based access profile, which lists the exact groups and applications to grant.	System Administrator	☐
5.4	**Create the identity** The System Administrator creates the account in the identity provider with a unique username and a temporary password that must be changed at first login.	System Administrator	☐
5.5	**Provision mailbox and calendar** The System Administrator provisions the new hire's mailbox, calendar and shared distribution list memberships defined in the access profile.	System Administrator	☐
5.6	**Assign security groups** The System Administrator adds the account to the security groups and distribution lists listed in the access profile for the new hire's role.	System Administrator	☐
5.7	**Provision application access** The System Administrator grants access to the ticketing system, file shares and business applications named in the access profile, and nothing beyond that list. **Checkpoint:** The granted access matches the role-based access profile exactly, with no extra applications or admin rights added.	System Administrator	☐

Step	Task	Owner	Done
5.8	**Configure MFA enrollment** The System Administrator sends the new hire an MFA enrollment link tied to the temporary password and confirms enrollment is required before the account can sign in to company applications. **Warning:** Never share an MFA enrollment link or code over an unverified channel; confirm the recipient's identity first.	System Administrator	☐
5.9	**Notify the hiring manager and HR** The Service Desk Analyst notifies the hiring manager and HR Coordinator that the accounts are ready and shares the credential delivery plan.	Service Desk Analyst	☐
5.10	**Deliver credentials securely** The Service Desk Analyst sends the username and the temporary password through two separate channels, such as a portal message and a phone call, never in the same email. **Warning:** Sending a username and temporary password together in one message defeats the purpose of separate verification.	Service Desk Analyst	☐
5.11	**Confirm first login and MFA** On day one, the Service Desk Analyst confirms with the new hire that they logged in, changed the temporary password and completed MFA enrollment. **Checkpoint:** The new hire has signed in, changed the password and enrolled MFA before being marked ready to work.	Service Desk Analyst	☐
5.12	**Log the account in the access register** The Service Desk Analyst records the account details, access profile and creation date in the access register or asset management system.	Service Desk Analyst	☐
5.13	**Close the onboarding ticket** The Service Desk Analyst closes the ticket once the account, access and MFA enrollment are all confirmed working, and archives the approval documentation.	Service Desk Analyst	☐

6. Quality checks

- New hires have working login, email and required application access before the start of their first day.
- Access granted matches the role-based access profile exactly, with no extra permissions added.
- MFA is enrolled before the account is used to access any company application.
- Every onboarding ticket includes documented manager approval before account creation.

7. Records

- Approved onboarding request ticket
- Access register entry for the new account
- MFA enrollment confirmation
- Credential delivery confirmation

8. KPIs

- Percentage of accounts ready before the new hire's start date
- Average time from approval to completed provisioning
- Number of access exceptions found during later access reviews

9. Common mistakes

- Creating the account before manager approval is attached to the ticket.
- Copying an existing employee's access instead of using the role-based access profile.
- Sending the username and temporary password in the same message.
- Forgetting to require MFA enrollment before the account can sign in.
- Leaving the ticket open after the account and access are confirmed working.

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.