

Software Access Request

IT Helpdesk — New Employee Onboarding

Last reviewed: March 2026

OVERVIEW

Document Summary

SOP ID	SOP-IT-004	Version	1.2
Department	IT Helpdesk	Last Reviewed	March 2026
Owner	IT Team Lead	Status	Active

PURPOSE

Why this SOP exists

To ensure new employees receive the correct system access on their first day, without delays or security exceptions.

SCOPE

What this SOP covers

This SOP applies to all IT helpdesk staff processing access requests for new full-time employees. It does not cover contractor access or role changes.

DEFINITIONS

Key Terms

Access request	A ticket submitted by a hiring manager via the HR portal confirming a new hire's role, start date, and req
Provisioning	The process of creating user accounts and assigning permissions in each system.
RBAC	Role-based access control — the framework used to assign permissions by job function.

ROLES

Who does what

IT Helpdesk Analyst	Processes the request and provisions access.
IT Team Lead	Reviews and approves requests flagged for elevated permissions.
HR	Submits the access request and confirms role details.

TOOLS

What you need before starting

HR Portal	Access requests from hiring managers.
Identity Management System	User provisioning and permissions assignment.
IT Ticketing System	Logging, audit trail, and ticket closure.

PROCEDURE

Step-by-Step Instructions

01**Verify the access request**

Log into the HR portal and locate the new hire's access request. Confirm the employee's name, start date, role, and required systems match what is on file.

Note: If any details are missing or inconsistent, return the request to HR for correction before proceeding.

02**Provision access**

Open the identity management system and create a new user profile using the employee's legal name and company email. Assign permissions using the RBAC template for their role.

Note: Do not grant elevated permissions without IT Team Lead approval.

03**Confirm and log**

Send the employee a confirmation email with login instructions and their temporary password. Log the completed request in the IT ticketing system, including the date, systems provisioned, and your name.

Note: Close the ticket once all systems have been confirmed and the log entry is complete.

COMPLIANCE

Governance and Requirements

This procedure supports SOC 2 compliance requirements for access control and least-privilege provisioning. All access requests must be logged and traceable.

RECORDS

Logging Requirements

All completed access requests must be logged in the IT ticketing system and retained for a minimum of 12 months.

REVISION HISTORY

Change Log

Version	Date	Changed by	Summary
1.0	Jan 2025	J. Park	Initial version
1.1	Sep 2025	M. Torres	Added RBAC template reference
1.2	Mar 2026	J. Park	Updated retention period to 12 months