STANDARD OPERATING PROCEDURE

User Access Review SOP

Document no.	SOP-IT-008
Revision	1.0
Owner	IT Security Manager
Effective date	September 15, 2026
Review cycle	Every 6 months

1. Purpose

To periodically verify that user access to systems and data remains appropriate, removing excess or stale permissions and confirming access still matches each person's current role.

2. Scope

Applies to scheduled reviews of user accounts, group memberships and application access across in-scope systems, including leavers and role changes. Initial account creation and password resets are covered by separate procedures.

Definitions

Access review cycle	A scheduled point-in-time review of who has access to a given system.
Entitlement	A specific permission or group membership granted to a user account.
Segregation of duties	A control that prevents one person from holding two conflicting entitlements, such as creating and approving the same transaction.
Stale account	An account with no recent login activity that may no longer be needed.

3. Responsibilities

System Administrator	Generates access reports, revokes or adjusts access, and disables stale accounts.
IT Security Manager	Coordinates the review cycle, resolves flagged conflicts, and reports results.
Application Owner	Certifies whether each user's access to their application is still needed.
People Manager	Confirms which team members still need access based on current role and team changes.

RACI matrix

Activity	System Administrator	IT Security Manager	Application Owner	People Manager
Generate and distribute the access review	R	R/A	I	I
Certify user access decisions	I	C	R/A	R
Revoke or adjust access	R/A	C	I	I
Resolve segregation of duties conflicts	C	R/A	C	I

Activity	System Administrator	IT Security Manager	Application Owner	People Manager
Report review completion to leadership	I	R/A	I	I

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

4. Materials and PPE

Materials, tools and systems

- Identity provider reporting tool
- Access review spreadsheet or template
- Segregation of duties matrix
- Review calendar
- Reviewer sign-off or attestation record

5. Procedure

Step	Task	Owner	Done
5.1	**Generate the access review report** The System Administrator exports a list of users and their entitlements for each system in scope from the identity provider.	System Administrator	☐
5.2	**Distribute the review to reviewers** The IT Security Manager sends each access list to the relevant Application Owner or People Manager, with a deadline for completing the certification.	IT Security Manager	☐
5.3	**Certify each user's access** The Application Owner or People Manager reviews the list and marks each user's access as still needed, to be modified, or to be removed. **Checkpoint:** Every account on the list receives an explicit decision; none are left blank or skipped.	Application Owner	☐
5.4	**Flag segregation of duties conflicts** The IT Security Manager reviews certified decisions against the segregation of duties matrix and flags any user holding conflicting entitlements.	IT Security Manager	☐
5.5	**Identify leavers and role changes** The System Administrator cross-checks the access list against recent departures and internal role changes to catch access that should already have been removed. **Warning:** Any active account for a departed employee is a priority removal and should not wait for the next scheduled review.	System Administrator	☐
5.6	**Revoke or adjust access** The System Administrator implements each reviewer's decision, removing or adjusting entitlements as certified.	System Administrator	☐
5.7	**Disable stale accounts** The System Administrator disables or removes accounts with no recent login activity, after confirming the account is not a required service account. **Checkpoint:** Each stale account is confirmed as not a required service account before it is disabled.	System Administrator	☐

Step	Task	Owner	Done
5.8	**Document review decisions** The IT Security Manager records each reviewer's decisions and any supporting notes in the access review record.	IT Security Manager	☐
5.9	**Escalate contested decisions** The IT Security Manager reviews and makes the final call on any decision the reviewer and account holder disagree about.	IT Security Manager	☐
5.10	**Compile completion and sign-off** The IT Security Manager compiles the completed review results and collects sign-off confirmation from each reviewer.	IT Security Manager	☐
5.11	**Report to leadership** The IT Security Manager reports the review's completion rate and notable findings, such as segregation of duties conflicts, to leadership.	IT Security Manager	☐
5.12	**Schedule the next cycle** The IT Security Manager schedules the next access review cycle and updates the review calendar.	IT Security Manager	☐

6. Quality checks

- Every account on the review list receives an explicit reviewer decision.
- Access for departed employees is revoked promptly rather than waiting for the next cycle.
- Segregation of duties conflicts are documented and resolved.
- Each review cycle has a signed-off completion record.

7. Records

- Access review report
- Reviewer certification or sign-off
- Segregation of duties exception log
- Revocation confirmation

8. KPIs

- Access review completion rate
- Average time to revoke access after a role change or departure
- Number of stale or excess access findings per cycle
- Percentage of accounts with no reviewer response

9. Common mistakes

- Rubber-stamping the review without checking each account individually.
- Missing internal role changes because the focus is only on leavers.
- Leaving a flagged segregation of duties conflict unresolved after the review closes.
- Not revoking access promptly once a reviewer marks it for removal.

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.