IT account provisioning and access requests

Manual | 10 steps | 3 roles | Created Sep 2, 2026 | Updated Sep 2, 2026 | v1

How IT grants, reviews, and removes system access for staff, keeping every request approved and privileges minimal.

TRIGGER

When a manager requests access for a team member, or when a role change alters what someone needs.

10 STEPS

1 **Requesting Manager submits the request naming the person, the system, the access level, and the business reason.**

The business reason is not bureaucracy. It is what lets anyone later judge whether the access is still needed, and requests without one cannot be reviewed.

2 **IT Administrator confirms the request came from that person's actual manager.**

Requests arriving from the person who wants the access, or from a colleague acting helpfully, are the most common route to unauthorised access. Verify through a known channel, never by replying to the request itself.

Verified: Go to step 3: IT Administrator checks whether the requested level is privileged or grants access to customer data.
Cannot verify: Go to step 10: IT Administrator records the request as denied with the reason and informs the Requesting Manager.

3 **IT Administrator checks whether the requested level is privileged or grants access to customer data.**

Standard access: Go to step 5: IT Administrator grants the minimum access that satisfies the stated reason, using a role or group rather than individual permissions.
Privileged or customer data: Go to step 4: System Owner reviews and approves the request, and records that approval.

4 **System Owner reviews and approves the request, and records that approval.**

A second approver for privileged access, recorded. This is the control an auditor tests, and it only exists if the record does.

Approved: Go to step 5: IT Administrator grants the minimum access that satisfies the stated reason, using a role or group rather than individual permissions.
Denied: Go to step 10: IT Administrator records the request as denied with the reason and informs the Requesting Manager.

5 **IT Administrator grants the minimum access that satisfies the stated reason, using a role or group rather than individual permissions.**

Groups over individual grants. Individually granted permissions are invisible in aggregate and nearly impossible to review later.

6 **IT Administrator records the grant: who, what system, what level, who approved, and the date.**

> This record is what makes the periodic review in step 8 and offboarding possible at all. Without it both become guesswork.

7 **IT Administrator confirms the access works and notifies the Requesting Manager, without sending credentials over an unencrypted channel.**

> Never send a password by email or chat. Use a first-login reset or your password manager's sharing mechanism.

8 **System Owner reviews all access to their system on a defined cadence and confirms each grant is still needed.**

Quarterly

> The reviewer has to be the person who understands what the access does, not IT. IT can produce the list but cannot judge necessity.

All still required: Ends the procedure
Access no longer needed: Go to step 9: IT Administrator revokes the unneeded access and records the revocation and its date.

9 **IT Administrator revokes the unneeded access and records the revocation and its date.**

> Revocations are recorded exactly like grants. "When was this removed" is asked as often as "who approved this".

Revoked: Go to step 8: System Owner reviews all access to their system on a defined cadence and confirms each grant is still needed.

10 **IT Administrator records the request as denied with the reason and informs the Requesting Manager.**

Record denials too. A denied request that is resubmitted through a different route is a signal worth being able to see.

Recorded: Ends the procedure

ROLES INVOLVED

Requesting Manager · IT Administrator · System Owner

REVIEW CADENCE

Annually, and immediately after adding a system that holds customer data or after any access-related incident.

Name the person accountable for this procedure before you put it into use.

CHANGE THESE BEFORE YOU USE IT

- Define what counts as privileged in step 3 for your systems, explicitly and in writing. Left vague, everything becomes standard access.
- Name your actual request channel. A procedure that says "submits the request" without naming where will be bypassed by chat messages.
- Set the review cadence in step 8 per system rather than uniformly. Customer data monthly and an internal wiki annually is more realistic than quarterly for everything.
- If you use single sign-on and an identity provider, most of steps 5 to 7 become group membership changes, and the procedure gets shorter and more reliable.
- Connect this to your offboarding procedure so the grant record in step 6 is the checklist used on someone's last day.

This is a free starting point from sendabrief.com, not compliance advice. It is written to be adapted.

Source: https://sendabrief.com/templates/it-account-provisioning