

Staff and volunteer access lifecycle

Make joining, changing roles and leaving a repeatable process with approval, ownership and verification.

Purpose

Give each access change a trigger, an approver and a completion check. Include staff, volunteers, temporary helpers and service providers without relying on someone's memory of every account.

Prepare before the discussion

- Role definitions, application owners and the authoritative staff or volunteer roster.
- A list of accounts, devices, badges, shared mailboxes and provider access.
- The join, change and leave notification process and available verification evidence.

Review prompts - first half

1. Name the trigger and owner

Define who notifies IT or the system owner about a join, role change or departure, and how an urgent departure is handled.

2. Define role-based access

Document the access a role needs and who approves exceptions. Use individually attributable accounts where the service supports them.

3. Check administrative access

Approve privileged access separately and record its business need, MFA and review owner. Keep recovery secrets in the approved protected store.

4. Prepare the working environment

Confirm device ownership, support boundaries, required sign-in methods and the person's training and reporting contacts.

5. Complete the joining check

Verify that the person can use the approved services and cannot reach a representative restricted area. Use authorized, non-disruptive checks.

Review prompts - continued

6. Treat a role change as removal and approval

Remove obsolete access before adding the new role's permissions. Include group membership, delegated access, exports and shared resources.

7. Close access after departure

Address accounts, active sessions, recovery methods, provider access, devices and physical credentials through the approved offboarding process.

8. Preserve necessary business records

Assign mailbox and file ownership, retention and lawful preservation decisions before disposing of records. Do not transfer personal data without an approved purpose.

9. Verify a representative case

Check the completed record against the current application inventory. Record evidence of removal and any service limitations or follow-up work.

10. Review seasonal and shared roles

Reconcile volunteer rotations, event accounts, shared devices and dormant access. Give temporary access an end date and a named reviewer.

Useful outputs

- A join, change and leave checklist with named approvers and system owners.
- A redacted completion record for a representative role change or departure.
- An exception register with a responsible owner and review date.

Review prompt

Apply at every join, role change and departure; reconcile access on an agreed recurring cadence.

Your next decisions

Use this worksheet in your approved protected workspace. Record categories and decisions, not personal records, passwords, card data or recovery codes.

Scope / systems / programs: _____

Review owner: _____ Review date: _____

Topic / gap	Evidence / unknown	Owner / next action	Due / completion check

Where Layer8 can help

Managed IT: Maintain the agreed environment and put repeatable operating procedures in place.

Scope and use

Agree timing, employment and record-preservation decisions with the responsible organizational owners. This checklist does not require submitting account credentials or personal rosters to Layer8.

Original Layer8 preparation prompts. Linked reference organizations do not endorse this guide.

Primary references

CISA: small and medium business resources

<https://www.cisa.gov/small-and-medium-sized-business-resources>

NIST: CSF quick-start guides

<https://www.nist.gov/cyberframework/quick-start-guides>

Online edition: [Layer8 resource library / access-lifecycle](#)