JOINERS, MOVERS & LEAVERS

Staff access change workbook

Use one copy per access change. Confirm the requester and authority through an established channel. Keep personal details and completed records in the approved private location.

Organisation / reference	Owner / role	Date / review

CHECK TOGETHER. RECORD THE GAPS.

- [ ] **Verify the request**
  Confirm the authorised requester, change type, effective time and the person or role affected.
- [ ] **Agree the access list**
  Identify required systems, groups and data access with each system owner; avoid copying unrelated permissions.
- [ ] **Check elevated access**
  Review administrator roles, shared access and any approved time-limited exceptions separately.
- [ ] **Prepare the device**
  Agree device allocation or return, enrolment, approved software and ownership of business data.
- [ ] **Complete the account changes**
  Create, adjust or remove access at the approved time. Review MFA and recovery arrangements where relevant.
- [ ] **Review remaining access**
  For a departure or reduced role, check sessions, integrations and remote access; rotate affected shared secrets through the approved process.
- [ ] **Confirm and record**
  Record the changes, exceptions, owner confirmation and any remaining action without storing passwords here.

Ticked boxes record your review; they do not certify compliance. Do not enter passwords, recovery codes or private configuration here.

DECISIONS, ACTIONS & EVIDENCE

Make the next step clear.

Complete locally in a PDF reader or print for a discussion. Keep the completed copy in your approved private record system.

Request and effective time

Change type, authorised request reference, role and effective date/time with time zone.

Systems and permissions

System owner, required access, removed access and device or licence actions.

Approvals and exceptions

Record authority, business data handover and any time-limited exception with its review date.

Completion and evidence

Completion reference, checks performed, unresolved actions and confirming owner.

RELATED POLICY / GUIDANCE

Identity & access

Endpoints & devices

Retention & disposal

ASD/ACSC: Engaging a managed service provider