

Access Control Policy

Owner	[Security owner role]
Approved by	[Policy approver role]
Effective date	[Effective date]
Next review	[Next review date]
Version	[Version]

1. Purpose and scope

This policy supports the SOC 2 common criteria CC6.1, CC6.2 and CC6.3 by ensuring access to systems and data is restricted to authorized individuals.

This policy applies to all [In-scope personnel] and [In-scope systems].

2. Identity and authentication

- Unique user IDs: All users are assigned a unique ID. Shared accounts are prohibited.
- Passwords: A password used as the only factor is at least [Minimum password length] characters long. Passwords are managed in [Identity provider] or the Company password manager, and are changed when there is evidence of compromise rather than on a fixed schedule.
- Multi-factor authentication (MFA): MFA is required for all critical systems, including [Cloud provider] and [Identity provider].

3. Requesting and approving access

- Access to an in-scope system is requested in [Ticketing system] and approved by the system owner or the requester's manager before it is granted.
- The person who approves access is never the person who receives it.
- Access is granted by role. Access beyond the role records a reason and an end date.

4. Authorization and access management

- Least privilege: Access is granted based on the principle of least privilege.
- Provisioning and deprovisioning: Formal processes are used to grant, modify, and revoke access in a timely manner. Access is removed within 24 hours of termination.

- Access reviews: User access to in-scope systems is reviewed at least every six months, and access to production and privileged roles at least quarterly. The reviewer is not the person who granted the access, and each review records a keep, reduce or remove decision for every account.

5. Privileged access

Privileged access is restricted to named individuals, requires separate admin accounts, and is reviewed quarterly.

Administrative actions in production are logged, and the logs are kept under the Logging and Monitoring Policy.

6. Joiners, movers and leavers

- Joiners: accounts are created only after the [Human resources system] shows a start date and the access request is approved.
- Movers: when a person changes role, access the new role does not need is removed within 5 business days.
- Leavers: the identity provider account is disabled and live sessions are revoked within 24 hours of the termination date. Access to systems outside single sign-on is removed under the offboarding checklist, and each removal is recorded with its date.

7. Service accounts

Each service account has a named human owner, is used only by the system it serves, and has its credential stored in the secrets manager. The credential is rotated when someone who could read it leaves the Company.

8. Roles and responsibilities

Role	Held by	Responsibility
Policy approver	[Policy approver role]	Approves this policy, each new version, and any risk the Company accepts instead of meeting it.
Policy owner	[Security owner role]	Maintains this policy, makes sure the controls in it operate, keeps the evidence, and reviews it at least once a year.
System owners	[Engineering owner role]	Approve access requests for their systems and take part in access reviews.
All personnel	Everyone in scope	Follow this policy and report a suspected breach of it to the [Security owner role].

9. Evidence and records

The records below show that this policy operates. Each is dated, kept for at least [Evidence retention period], and stored where an auditor can be given it.

Record	What it shows	Where it is kept
Approved policy	This document, signed by the approver, with its version history.	[Documentation system]
Access review report	Certifications of user access reviews.	[Evidence storage location]
MFA policy configuration	Screenshot of MFA enforcement settings.	[Identity provider]
Deprovisioning records	Evidence of timely access revocation.	[Human resources system]
Access requests	Tickets showing approval before access was granted.	[Ticketing system]
Offboarding checklists	Termination date beside the date each access was removed.	[Evidence storage location]

10. Exceptions and enforcement

A deviation from this policy needs a written exception approved by the [Security owner role] before it begins. Each exception records the rule not met, the business reason, the compensating control and an expiry date no more than 12 months away. Exceptions are reviewed at each annual review.

A breach of this policy is handled under the Company disciplinary process and may lead to action up to and including termination of employment or contract. A breach that exposes customer data is also handled as a security incident.

11. Review and approval

The [Security owner role] reviews this policy at least once a year and after any significant change to the business, the systems in scope or the risks they face. The [Policy approver role] approves each version. Personnel are told of material changes and acknowledge the current version.

Version	Date	Summary of change	Approved by
[Version]	[Effective date]	First version.	[Policy approver role]

Policy approver

Name:

Signature:

Date:

12. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

Field	What to enter
[Company name]	Your legal company name.
[Effective date]	The date the approver signs this version.
[Version]	Start at 1.0 and increase it each time the document changes.
[Security owner role]	The role that runs the security program day to day, for example Chief Technology Officer.
[Policy approver role]	The officer who approves policies and accepted risks, for example Chief Executive Officer.
[Evidence storage location]	The shared folder or system where evidence is kept.
[Documentation system]	Where policies and procedures are published, for example the company wiki.
[In-scope personnel]	Who the policy covers, for example employees and contractors with access to company systems.
[In-scope systems]	The product, cloud accounts and tools inside the audit boundary.

Field	What to enter
[Identity provider]	The single sign-on directory, for example Google Workspace or Okta.
[Cloud provider]	Where production runs, for example AWS, Google Cloud or Azure.
[Minimum password length]	At least 15 characters where a password is the only factor.
[Human resources system]	Where start and end dates are recorded.
[Ticketing system]	Where changes and incidents are tracked, for example Jira or Linear.
[Evidence retention period]	How long audit evidence is kept, for example three years.
[Engineering owner role]	The role that owns production systems, for example engineering lead.
[Next review date]	The date this version must be reviewed by, at most 12 months after the effective date.

Source

Source: free template from www.polaralabs.com/templates/access-control-policy (CC BY 4.0).