

Access Control Policy

Purpose

Granting the right access to the right people at the right time — and no more — is foundational to protecting Your Organization information. This policy defines the principles, roles, and processes Your Organization uses to grant, review, and revoke access to its information systems and data.

Scope

This policy applies to all Your Organization information systems, applications, and data stores, including cloud services, SaaS tools, developer infrastructure, network devices, databases, and physical access systems. It applies to all workforce members, contractors, and third-party users.

Principles

- **Least privilege.** Users receive the minimum level of access required to perform their duties. Broad or standing administrative access is discouraged and must be justified.
- **Need to know.** Access to sensitive data is granted only to those with a documented business need.
- **Separation of duties.** Critical functions are split across multiple users where feasible so no single individual can complete a sensitive transaction unilaterally (e.g. request vs. approve).
- **Role-based access control (RBAC).** Access is granted via roles aligned to job function, not to individuals. Roles are the unit of provisioning, review, and revocation.
- **Authenticate before authorize.** Every access decision is preceded by strong authentication (see the Password and Authentication Policy).

Roles and responsibilities

- **Data and System Owners.** Define the roles available on their systems, approve role assignments, and review access quarterly.
- **IT and Security Operations.** Provision, modify, and deprovision access according to approved tickets; maintain authoritative audit logs.
- **People Operations.** Notify IT promptly of all new hires, role changes, and terminations so access can follow the worker.
- **Managers.** Certify their direct reports' access during quarterly reviews and attest to ongoing need.

Account lifecycle

Provisioning

New accounts are created from an approved access request, tied to an authoritative HR record, and assigned only the roles approved by the data owner. MFA is enrolled before first substantive use.

Transfer

When a user changes roles, their previous access is removed and the new role assigned — access is not additive across roles absent an explicit business need and owner approval.

Deprovisioning

On termination, all Your Organization access must be disabled within one business day (same day for involuntary terminations). Federation accounts, local accounts, SSH keys, and API tokens owned by the user are all in scope. Accounts remain disabled (not deleted) for a retention period defined in the Data Retention Policy before final removal.

Privileged access

Privileged accounts (domain admin, cloud root, production database admin, production deploy, secrets management admin) receive the strongest controls:

- Separate, named privileged accounts — no shared root credentials.
- MFA is mandatory on every authentication.
- Privileged sessions are logged and reviewed.
- Just-in-time elevation is used where the tooling supports it.
- Credentials are vaulted and rotated on schedule and immediately on a leaver event.

Service accounts

Service accounts (non-human identities) must have a named human owner, a documented purpose, the minimum permissions required, no interactive login rights, and long credentials that are rotated on schedule. Service-account credentials must never be stored in source code or in unmanaged locations.

Access reviews

Your Organization conducts access reviews at least **quarterly** for privileged and high-sensitivity roles, and at least annually for all other access. Managers certify their direct reports' access; data owners certify external or cross-team access. Findings are tracked to closure.

Remote and vendor access

Remote workforce access uses Your Organization-approved VPN or zero-trust access with MFA. Vendor access is time-bound, scoped to what the contract covers, and approved by the system owner and security.

Scope exceptions

Exceptions must be submitted in writing, document the business justification and compensating controls, and be approved by the CISO or designee. Exceptions are time-bound and reviewed on expiration.

Review cadence

This policy is reviewed annually by the Information Security team, with input from IT Operations and People Operations, or sooner if a material change to identity infrastructure or applicable regulation occurs.

Effective date: [the date this policy takes effect]