

Personnel Security Policy

Purpose

Trust in the people who access Your Organization systems and data is established before day one and maintained throughout their tenure. This policy defines the screening Your Organization performs before granting access to sensitive systems, and the security steps taken when a workforce member changes role or leaves the organization.

Scope

This policy applies to all prospective and current Your Organization workforce members — employees, contractors, and interns — whose role provides access to company systems, Confidential or Restricted data, or facilities housing information systems.

Pre-employment and pre-engagement screening

- Roles with access to Confidential or Restricted data, financial systems, or production infrastructure undergo background screening appropriate to the role and permitted by applicable law, completed before or promptly after start date and before access to sensitive systems is granted.
- Contractors and third-party personnel performing equivalent functions are subject to equivalent screening requirements, either performed directly or attested to by their employer under contract.
- Screening scope and depth are proportionate to role sensitivity, determined jointly by People Operations and Information Security.

Confidentiality and acceptable use commitments

All workforce members acknowledge Your Organization's confidentiality obligations and the Acceptable Use Policy as a condition of access, at onboarding and upon material policy updates.

Role transfers

When a workforce member changes role, People Operations notifies IT and the relevant system owners so that access can be adjusted — new access provisioned for the new role, and access tied to the prior role removed rather than accumulated. Elevated or sensitive access carried over from a prior role requires fresh approval from the new role's data or system owner.

Termination and offboarding

- People Operations notifies IT of all terminations — voluntary and involuntary — with enough lead time for same-day access revocation on the termination date, and immediate revocation for involuntary

terminations.

- Offboarding includes: disabling accounts and access, retrieving company-owned equipment and badges, revoking physical access credentials, and reminding the departing individual of ongoing confidentiality obligations.
- For involuntary terminations or terminations involving elevated risk, Information Security and People Operations coordinate on timing and sequencing (e.g., access revocation concurrent with or immediately preceding notification) to minimize risk.
- Offboarding completion is tracked to closure and periodically audited against HR termination records to catch gaps.

Sanctions

Violations of Your Organization security policy by a workforce member are addressed through the standard People Operations disciplinary process, proportionate to the severity and intent of the violation, up to and including termination.

Roles and responsibilities

- **People Operations.** Owns screening execution, onboarding/offboarding process, and disciplinary process coordination.
- **IT and Security Operations.** Executes access provisioning and revocation based on People Operations notifications.
- **Managers.** Notify People Operations promptly of role changes and departures affecting their direct reports.

Review cadence

This policy is reviewed annually by People Operations and Information Security, or sooner following a change in applicable screening law or an offboarding-related incident.

Effective date: [the date this policy takes effect]