

Security Awareness and Training Policy

Purpose

People are both Your Organization's strongest control and its most targeted attack surface. This policy establishes Your Organization's security awareness and training program, ensuring every workforce member understands their security responsibilities and that individuals in higher-risk roles receive training tailored to the risks they manage.

Scope

This policy applies to all Your Organization workforce members — employees, contractors, and interns — with access to company systems or data, regardless of role or tenure.

General security awareness

- All workforce members complete security awareness training as part of onboarding, before or immediately upon being granted system access.
- All workforce members complete annual refresher training covering current threats (phishing, social engineering, credential theft), acceptable use expectations, data handling, and incident reporting.
- Awareness content is supplemented throughout the year with simulated phishing exercises, security bulletins, and just-in-time reminders tied to observed risk trends.

Role-based training

- Workforce members in roles with elevated risk exposure — engineers, administrators with privileged access, personnel handling regulated or Restricted data, and people managers — receive additional role-specific training aligned to the risks their role introduces (e.g., secure coding for engineers, privileged access hygiene for administrators, data handling obligations for regulated-data custodians).
- Role-based training needs are identified during onboarding and reassessed when a workforce member changes role or gains new system access.
- Completion of role-based training is tracked and factored into access provisioning for sensitive systems where applicable.

Insider threat awareness

All workforce members receive training on recognizing and reporting indicators of insider threat — data exfiltration behavior, unauthorized access attempts, and social engineering targeting internal processes — as part of onboarding and annual refreshers. Reporting channels are communicated clearly, including how to report anonymously where Your Organization policy supports it.

Specialized audiences

- **Incident responders** receive training and participate in tabletop exercises per the Incident Response Plan.
- **Executives and finance personnel** receive targeted training on business email compromise and wire-fraud social engineering given their elevated targeting risk.
- **New managers** receive training on the security aspects of onboarding and offboarding their direct reports, coordinated with People Operations.

Training records

People Operations and Information Security jointly maintain records of training assignment and completion, including dates and content version. Records support audit and compliance evidence requests and inform where the program needs reinforcement.

Non-completion

Workforce members who do not complete required training within the assigned window are subject to escalating reminders and, for extended non-completion, restriction of system access until training is completed, at the discretion of People Operations and Information Security.

Roles and responsibilities

- **Information Security.** Owns training content, phishing simulation program, and role-based curriculum design.
- **People Operations.** Owns onboarding logistics, training assignment, and completion tracking.
- **Managers.** Ensure their direct reports complete required training on schedule.

Review cadence

This policy and the underlying training curriculum are reviewed annually by Information Security and People Operations, or sooner following a significant incident with a training-related root cause or a material shift in the threat landscape.

Effective date: [the date this policy takes effect]