

Security Awareness Training 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 sets how [Company name] (the "Company") screens, trains and holds accountable the people who work for it. It supports the SOC 2 common criteria CC1.4 and CC1.5 by defining security requirements throughout the employee lifecycle.

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

2. Onboarding and employee conduct

- Background checks: Background checks are completed for new hires before they receive access to customer data, where the law allows.
- Confidentiality: All employees must sign a confidentiality agreement.
- Acceptable use: Personnel must adhere to the Acceptable Use Policy.
- Standards of conduct: All personnel acknowledge the general standards of conduct in the Acceptable Use Policy at hire and each year.

3. Who is trained and when

Audience	Training	Deadline
All new employees and contractors with access to Company systems	Full curriculum in section 4, plus the Acceptable Use Policy and the information security policies	Within 30 days of their start date
All employees and contractors	Full curriculum in section 4, refreshed with any new threats, incidents or policy changes from the past year	Once every 12 months

Audience	Training	Deadline
Engineers and anyone with production access to the production cloud environment	Secure development topic in section 4, in addition to the full curriculum	Within 30 days of being granted production access, then once every 12 months
Anyone involved in a security incident caused by human error, or who fails a phishing simulation twice in a row	Targeted refresher on the relevant topic	Within 14 days

The [People owner role] tells the [Security owner role] of every new starter so that training is assigned in their first week. Access to Restricted data is not granted until the person has completed training.

4. What the training covers

Topic	What it covers
Phishing and social engineering	Recognizing phishing emails, texts and calls; checking sender and link details; payment and gift card fraud; reporting a suspected phish instead of deleting it.
Passwords and multi-factor authentication	Unique passwords for every account; using the Company password manager; enabling multi-factor authentication; never sharing credentials or approving unexpected login prompts.
Data classification and handling	The four levels in the Data Classification and Retention Policy; where Restricted and Confidential data may be stored and shared; keeping customer data from the Company's product out of personal accounts and public AI tools.
Device security	Keeping laptops updated and encrypted; screen lock; approved software only; working safely on public Wi-Fi; what to do with a lost or stolen device.
Acceptable use of company systems	Business use of the Company's approved systems; limited personal use; monitoring; prohibited activity.
Incident reporting	What counts as an incident; how and where to report within 1 hour; not investigating alone; the no-blame reporting rule.
Physical and remote working security	Protecting screens and conversations in public and at home; locking devices away; handling visitors and printed material.
Secure development (engineers only)	The most common web application risks and how the Company prevents them; secrets management; code review; safe handling of production data in the production cloud environment.

5. Recording completion

Training is delivered through [Training method]. Every completion is recorded in the training log with the person, the training, the date and the result, and signed policy acknowledgments are filed with it. The [Security owner role] checks the log each month against the current staff list.

6. When training is overdue

1. A person who is overdue receives a reminder from the [Security owner role] with a 7-day deadline.
2. If still overdue after 7 days, the matter is escalated to their manager and the [People owner role].
3. If still overdue after 14 days, access to Restricted and Confidential data and to production systems is suspended until training is complete.
4. Repeated or deliberate non-completion is handled as a breach of the Acceptable Use Policy.

7. Performance management

Employee performance is formally reviewed at least annually to ensure competence and alignment with their responsibilities.

8. Sanctions

A disciplinary process, documented in [Disciplinary process document], is in place for violations of security policies.

9. Leaving the Company

When a person leaves, access is removed under the Access Control Policy and the offboarding checklist, Company equipment is returned, and confidentiality obligations continue after the last day.

10. 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.
People owner	[People owner role]	Runs background checks, onboarding, acknowledgments and the disciplinary process.
All personnel	Everyone in scope	Follow this policy and report a suspected breach of it to the [Security owner role].

11. 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]
Training completion	Records of security awareness training.	[Human resources system]
Signed acceptable use acknowledgment	Each person confirms the Acceptable Use Policy at hire and each year.	[Human resources system]
Background check confirmations	A completed check for each new hire, without the report contents.	[Human resources system]

12. 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.

13. 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:

14. 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.
[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.
[Human resources system]	Where start and end dates are recorded.
[Evidence retention period]	How long audit evidence is kept, for example three years.

Field	What to enter
[Training method]	How training is delivered, for example a recorded session with a quiz.
[Disciplinary process document]	Where the disciplinary process is written down, for example the employee handbook.
[People owner role]	The role that runs hiring and departures, for example head of people.
[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/security-awareness-training-policy (CC BY 4.0).