

[Company name]

Security Awareness Training Program

Owner	[Security owner role]
Approved by	[Policy approver role]
Effective date	[Effective date]
Next review	[Next review date]
Version	1.0

1. Purpose

This program makes sure everyone at [Company name] (the "Company") understands the security threats they face, the Company's security policies, and their own responsibilities for protecting customer and Company information. It also produces the record that shows each person was trained.

2. Who is trained and when

Audience	Training	Deadline
All new employees and contractors with access to Company systems	Full curriculum in section 3, plus the Code of Conduct and the information security policies	Within 30 days of their start date
All employees and contractors	Full curriculum in section 3, refreshed with any new threats, incidents or policy changes from the past year	Once every 12 months
Engineers and anyone with production access to the production cloud environment	Secure development topic in section 3, 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.

3. Curriculum

The Company builds its training from well-established free materials. The trainer may use equivalent materials, provided every topic below is covered.

Topic	What it covers	Free resource to use
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.	Google Phishing Quiz (phishingquiz.withgoogle.com)
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.	CISA Cybersecurity Awareness Program materials
Data classification and handling	The four levels in the Data Classification Standard; 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.	The Company's Data Classification Standard
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.	NIST 'Cybersecurity basics' for small business
Acceptable use of company systems	Business use of the Company's approved systems; limited personal use; monitoring; prohibited activity.	The Company's Code of Conduct
Incident reporting	What counts as an incident; how and where to report within 1 hour; not investigating alone; the no-blame reporting rule.	The Company's Incident Response Plan
Physical and remote working security	Protecting screens and conversations in public and at home; locking devices away; handling visitors and printed material.	UK NCSC 'Top Tips for Staff' e-learning
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.	OWASP Top 10

The [Security owner role] delivers the training live or as a recorded session with the materials above, and the [Engineering owner role] delivers the secure development topic. Each session ends with a short quiz; a pass mark of 80% is required, and a person who does not pass repeats the quiz.

4. Phishing simulation (optional)

The Company may run phishing simulations to measure and improve awareness. When it does, the [Security owner role] runs at least one simulation per quarter, approved in advance by the [Policy approver role].

- Simulations use realistic scenarios but do not use lures about pay, benefits, health, layoffs or a colleague's personal circumstances.
- Click and report rates are recorded for each campaign and reported as totals, not used to shame individuals.
- A person who clicks a simulated phish receives immediate feedback and, after two consecutive failures, the targeted refresher in section 2.

5. Recording completion

Every completion is recorded in the Training Log workbook with the person's name, role, training type, date completed, quiz score and the trainer. Signed acknowledgments of the Code of Conduct and security policies are filed with the log. The [Security owner role] keeps the log for at least 3 years, as it is the evidence auditors sample.

Location of the Training Log workbook:

The [Security owner role] checks the log at the start of each month against the current staff list from the [People owner role] and follows up on anyone who is overdue.

6. Non-completion

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 Code of Conduct.

7. Ownership and review

The [Security owner role] owns this program, keeps the materials current, and reports completion rates and phishing results to the [Policy approver role] at least twice a year. The program is reviewed at least once a year and after any incident caused by human error. The [Policy approver role] approves each new version.

Source

Source: free template from www.polaralabs.com/templates/security-awareness-program (CC BY 4.0).