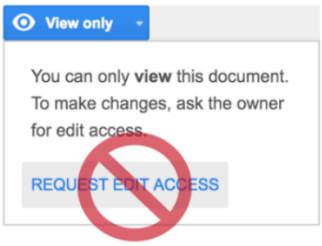
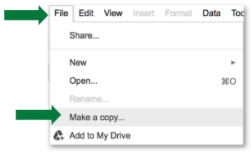
Strike Graph

Security Awareness and Training Policy Template



How to use this template:

This is a view-only file and cannot be edited. **Create your own copy** of this template to edit. In the menu, click **File > Make a copy...**



Strike Graph

Strike Graph Notes:

This template's purpose is to make sure everyone who uses your IT systems gets the right level of security awareness and role-based training. Strong evidence includes onboarding and annual training records, role-based course assignments, and phishing simulation results. A common pitfall is running one-off training without tracking participation, follow-up coaching, or documented refreshers after major system changes.

This template is intentionally simple, with bracketed fields like "[entity]" and "[entity specified frequency]" showing exactly where you customize names, owners, frequencies, and retention periods to match your organization.

Policy #:	Title:	Effective Date:
x.xxx	Security Awareness and Training Policy	MM/DD/YY

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications: NIST SP 800-53 – Awareness and Training (AT), NIST SP 800-12, NIST SP 800-16, NIST SP 800-50, NIST SP 800-100; Electronic Code of Federal Regulations (CFR): 5 CFR 930.301

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. SECURITY AWARENESS TRAINING

The [entity] shall:

a. Schedule security awareness training as part of initial training for new users.

b. Schedule security awareness training when required by information system changes and then [entity specified frequency] thereafter.

c. IT shall determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content shall:

   i. Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.

   ii. Address awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

2. SECURITY AWARENESS | INSIDER THREAT

IT Department shall:

a. Include security awareness training on recognizing and reporting potential indicators of insider threat.

3. ROLE-BASED SECURITY TRAINING

Strike Graph Notes:
For sections 1–3, decide who "IT Department" really is in your environment (e.g., "Information Security and IT Operations"), and set clear, defensible frequencies for awareness and role-based training. Ensure the curriculum covers core topics like phishing, password hygiene, incident reporting, and explicit insider threat awareness: how to recognize behavioral/red-flag indicators and how to report concerns safely. Align training scope to your real risks (e.g., CUI, PHI, PCI) and integrate with HR onboarding, your LMS, and any NIST 800-171/CMMC mappings.

IT Department shall:

a. Provide role-based security training to personnel with assigned security roles and responsibilities:

   i. Before authorizing access to the information system or performing assigned duties.

   ii. When required by information system changes and [entity specified frequency] thereafter.

b. Designate personnel to receive initial and ongoing training in the employment and operation of environmental controls to include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.

4. PHYSICAL SECURITY CONTROLS

Strike Graph Notes:
Tailor "physical security controls" to your actual environment: data center, wiring closets, office entrances, cages, colocation sites, and high-risk areas. Identify which teams need specialized training (facilities, security guards, on-site techs)

and reference any existing physical security policy. Gather access control procedures, vendor SLAs, and facility diagrams. Pitfalls include assuming facilities handles everything and not documenting that training is actually delivered and role-specific.

IT Department shall:

a. Provide initial and ongoing training in the employment and operation of physical security controls; physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures).

b. Identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.

5. PRACTICAL EXERCISES

Strike Graph Notes:
Define what “practical exercises” look like for you: phishing simulations for all staff, secure coding labs for developers, tabletop exercises for managers. Tie scenarios to your real threats and technologies instead of generic examples. Gather past incident data, risk assessments, and any existing simulation tools. Pitfalls include running one-off phishing tests without follow-up training or failing to document participation and outcomes for auditors.

IT Department shall:

a. Provide practical exercises in security training that reinforce training objectives; practical exercises may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for

security coding standards and processes.

6. SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

Strike Graph Notes:
Customize “specified staff” to named roles such as SOC analysts, help desk, admins, and managers who receive alerts or user reports. Describe the types of suspicious communications and anomalous behaviors relevant to your systems and CUI handling. Gather incident response plans, playbooks, and escalation procedures. A potential error is training only security staff and forgetting frontline users who actually see odd emails, logs, or system behavior first.

IT Department shall ensure that the information system:

a. Provide training to its specified staff on how to recognize suspicious communications and anomalous behavior in organizational information systems.

7. SECURITY TRAINING RECORDS

Strike Graph Notes:
You’ll want supporting evidence ready: LMS/exported reports of course completion, sign-in sheets for in-person sessions, copies of slide decks and training videos, phishing simulation results, insider-threat awareness campaigns, role-based training agendas, and documented procedures for how training is scheduled and assigned.

The [entity] shall:

a. Designate personnel to document and monitor individual information system security training activities including basic security awareness training and specific information system security training.

b. Retain individual training records for a [entity specified amount of time].

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests and confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY