Security Awareness Training Policy

CredX Tech Inc

September 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC1.4, CC2.2

1 Purpose and Scope

a. The purpose of this policy is to establish requirements for security awareness training to ensure that all personnel understand their responsibilities for protecting CredX's information assets and systems.

b. This policy applies to all full-time and part-time employees and contractors with access to CredX's systems or data.

2 Background

a. Human error and social engineering are among the leading causes of security incidents. A well-designed security awareness program reduces risk by ensuring personnel can recognize threats and respond appropriately. This policy establishes the minimum requirements for security education across the organization.

3 Policy

3.1 General Security Awareness Training

a. All employees and contractors must complete a security awareness training program:

   i. **New hires and new contractors** must complete the foundational security awareness training within **5 business days** of starting. System access may be restricted until training is confirmed complete.

   ii. **All personnel** must complete a refresher security awareness training at least **annually**.

   iii. Training completion must be tracked and recorded in the Policy Training Ledger maintained by HR and IT.

b. The annual security awareness training must cover, at minimum:

   i. Information security policies and acceptable use expectations.

   ii. Password hygiene and the use of multi-factor authentication.

   iii. Phishing and social engineering recognition and reporting.

   iv. Data classification and handling of sensitive and confidential information.

   v. Incident reporting procedures and what constitutes a security incident.

   vi. Physical security (clean desk, tailgating, visitor management).

   vii. Remote work security requirements.

viii. Consequences of policy violations.

3.2 Role-Based Security Training

a. Personnel in roles with elevated security responsibilities must complete additional role-based training:

   i. **Developers and engineers** must complete training on secure coding practices, OWASP Top 10, and secrets management at least annually.

   ii. **System administrators and IT staff** must complete training on privileged access management, patch management, and incident response at least annually.

   iii. **Managers and executives** must complete training on social engineering targeting leadership (e.g., business email compromise, spear phishing) at least annually.

3.3 Phishing Simulations

a. CredX must conduct simulated phishing exercises at least **twice per year** to assess employee susceptibility to phishing attacks.

b. Employees who fail phishing simulations must complete targeted remedial training within 5 business days.

c. Phishing simulation results must be reviewed by the ISM and used to update training content and focus areas.

3.4 Training Content and Program Management

a. The ISM is responsible for developing, maintaining, and updating the security awareness training program. Training content must be reviewed and updated at least annually to reflect current threats and organizational changes.

b. Training may be delivered via e-learning modules, instructor-led sessions, newsletters, or a combination of methods, provided that completion can be tracked and verified.

c. Training completion rates must be reported to the Leadership Team quarterly. Personnel who have not completed required training within the deadline must be escalated to their manager.

3.5 Non-Compliance

a. Employees and contractors who fail to complete required security awareness training within the defined timeframes may have their system access suspended until training is completed.

b. Repeated non-compliance may result in disciplinary action up to and including termination.