Security Culture Strategy – Overview Document

Summary

[List of changes 1](#_Toc202860237)

[Purpose 1](#_Toc202860238)

[Objectives 1](#_Toc202860239)

[Core Elements of Security Culture 1](#_Toc202860240)

[Key Activities and Initiatives 2](#_Toc202860241)

[Communication Channels 2](#_Toc202860242)

[Metrics to Track 2](#_Toc202860243)

[Recognition & Rewards 3](#_Toc202860244)

[Governance and Review 3](#_Toc202860245)

[Integration with ISO/IEC 27001 3](#_Toc202860246)

# List of changes

| Version | Description | Date | Author |
| --- | --- | --- | --- |
| 1.0 | First issue | 05.05.25 | Me |

# Purpose

This document outlines the strategy to define, build, and promote a strong security culture across the organization. A security culture ensures that all employees understand, value, and actively support information security.

# Objectives

* Align employee behavior with ISO/IEC 27001 policies and controls
* Encourage responsible and proactive attitudes toward information security
* Reduce human-related security risks through awareness and engagement

# Core Elements of Security Culture

* Leadership Commitment (ISO 27001 Clause 5.1)
* Employee Awareness and Training (Annex A.6.3)
* Clear and Accessible Policies (Annex A.5.1)
* Shared Values and Norms
* Accountability and Reporting

# Key Activities and Initiatives

| Activity | Description | Frequency | Owner |
| --- | --- | --- | --- |
| Security Onboarding | Mandatory briefing for new employees | First week | HR + CISO |
| Awareness Training | Role-based eLearning or instructor-led sessions | Annual | Security Team |
| Phishing Simulations | Test user response to simulated phishing emails | Quarterly | Security Team |
| Security Champions | Nominate and train champions across departments | Ongoing | Security Team |
| Internal Campaigns | Posters, newsletters, videos to raise awareness | Monthly | Communications |
| Incident Reporting | Easy and safe channels to report issues | Continuous | All Staff |
| Feedback & Surveys | Periodic pulse checks on security mindset | Biannual | GRC or Risk Team |

# Communication Channels

* Intranet Portal
* Company White Board
* Teams\Slack Announcements
* Digital Signage (screensavers, posters)

# Metrics to Track

* % of staff completing training
* % of staff passing phishing simulations
* # of security incidents reported by staff
* Employee feedback on security awareness
* # of contributions from Security Champions

# Recognition & Rewards

* Spot bonuses or gifts for employees who report real phishing emails
* Celebrate annual “Security Hero” award
* Create internal newsletters or events

# Governance and Review

* Strategy reviewed annually by CISO and GRC team
* Results presented in management review meetings (ISO 27001 Clause 9)
* Continuous improvement aligned with Clause 10 (Nonconformities and corrective actions)

# Integration with ISO/IEC 27001

This strategy supports the following Annex A controls:

* A.6.3 (Information security awareness, education, and training)
* A.5.1 (Policies for information security)
* A.5.36 (Contact with special interest groups)
* A.5.33 (Information security in project management)
* A.8.15 (Logging and monitoring – training users on what to report)

**Conclusion**

Building a security-aware culture is key to risk reduction, compliance, and trust. Everyone in the organization has a role to play in maintaining a secure working environment.

Generally security is an engaging topic, that fascinate people. We must try to push security related knowledge beyond work environment, highlighting the positive aspects in every-day life. For instance, to better understand cyber threats that could involves our children.