PKCERT

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2026

Essential Security Training Controls

NTISB

A. INTRODUCTION

1. Pakistan Information Framework: "**Essential Security Training Controls",** outlines the essentials of information security training controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

2. This Security Training framework applies to all employees, management, and relevant stakeholders of the organization. It establishes mandatory information security awareness, specialized role-based training, and continuous education requirements to ensure secure practices across all levels. The framework covers training design, delivery, documentation, and evaluation, ensuring compliance with regulatory obligations, alignment with risk management objectives, and adaptation to evolving threats and technologies.

B. SECURITY TRAINING CONTROLS

3. The organization shall establish and maintain a structured information security training program that defines priorities, topics, schedules, resources, delivery methods, and target audiences to ensure comprehensive coverage and program effectiveness aligned with organizational objectives and recommendations from NTISB, nCERT and sector regulator.

4. All senior management, employees and users shall complete mandatory information security awareness sessions before being granted system access, with annual refreshers and ad-hoc sessions conducted to address emerging threats, incidents, or regulatory changes.

5. Employees working in information security and IT shall receive role-specific training and obtain relevant certifications in information security and IT service management.

6. All personnel in high-risk or privileged roles (such as IT administrators, developers, incident responders, and forensic analysts etc.) shall complete specialized role-based security training, in addition to baseline awareness programs, as a condition for being granted system or data access.

7. Specialized training requirements shall be identified through risk assessments, audits, incidents, and regulatory obligations, and shall be refreshed periodically, at least annually.

8. Information Security training and awareness sessions shall address key areas, including but not limited to, password management, phishing, social engineering, secure remote work, mobile device security, data privacy, and incident reporting. These trainings and awareness sessions shall be delivered through multiple formats (e.g. e-learning, instructor-led sessions, webinars, tabletop exercises), with content reviewed and updated regularly.

9. All training participation shall be documented capturing attendee details, training dates, module names, and assessment outcomes, with records securely stored, backed up, and retained in accordance with regulatory and organizational requirements, and made available for audits or compliance checks.

10. The organization shall evaluate the effectiveness of its information security training and awareness program regularly through simulations, assessments, and performance monitoring, ensuring that outcomes directly update corrective and preventive actions.

11. The organization shall continuously strengthen its training and awareness program by incorporating feedback from employees, audits, and incident reviews, ensuring alignment with evolving threats and organizational needs.

PKCERT

Safeguarding Pakistan's Cyberspace

info@pkcert.gov.pk
www.pkcert.gov.pk