National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2026

Essential System and Communication Protection Controls

NTISB

A. INTRODUCTION

1. Pakistan Information security Framework: **"Essential System and Communication Protection Controls"**, outlines the baseline of information security system and communication protection controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

2. This framework applies to all organizational systems, networks, communication channels, and supporting technologies used to collect, transmit, process, or store information. It covers employees, third parties, and any other entities with access to organizational systems, ensuring secure design, implementation, and management of communication and system protections across the enterprise.

B. NETWORKS SECURITY

3. The organization shall establish, document, and formally approve network security requirements and ensure that approved security controls, in line with defense-in-depth principles and the organization's risk management strategy, are implemented and maintained to protect organizational networks.

4. The information security requirements for network security management shall include at least the following: -

a) Physical protection of all network infrastructure and information assets.

b) Appropriate segregation of networks across different environments and functions.

c) Appropriate perimeter security controls (like Firewall, IDS/IPS, etc. as per the requirements identified by the steering committee of information security).

d) Remote connectivity (on strict need basis) secured with appropriate measures, including VPNs, Time bound access, monitoring, auditing, and preferably multi-factor authentication.

e) Secure management of wireless networks, isolated from critical internal resources.

f) Systems with internet access are logically or physically segregated from critical information systems.

g) Network activity is logged and monitored to support incident investigation, security auditing, and compliance requirements

h) Establish and enforce change management and configuration management controls for all network changes and configuration updates.

C. PROTECTION OF ENDPOINT COMPUTING DEVICES

5. Information security requirements for protecting endpoint computing devices (Servers, workstations, desktops, laptops, mobile phones, tablets, etc.) shall be defined, documented, approved and implemented.

6. The information security requirements for protecting endpoint computing devices shall include at least the following:

a) Appropriate security solutions (anti-virus, anti-malware, EDR, XDR, etc.) depending upon the classification of asset and architecture of the organization. Endpoints shall not be left without any appropriate protection.

b) Establish and enforce controls governing the secure use of external or removable storage media to protect organizational information assets.

c) Maintain up-to-date endpoint computing devices through regular patch management and updates.

D. EVENT LOGS AND MONITORING

7. Information security requirements for event logs and monitoring shall be defined, documented, approved and implemented.

8. Event log and monitoring requirements shall include at least the following: -

a) Comprehensive event logging of, at a minimum, all critical assets, remote access connections and privileged user accounts.

b) Centralized log management and monitoring to aggregate, correlate, and continuously analyze cybersecurity events.

c) Retention of critical event logs for a minimum of 12 months for critical assets and for non-critical assets that impact critical assets; and for a minimum of 3 months for all other assets.

d) Systems synchronized clocks using NTP (Network Time Protocol).

e) Protection of active and archived logs from unauthorized tampering, destruction, or alteration, whether intentional or unintentional, to ensure their integrity and accuracy.

E. BACKUP AND RECOVERY MANAGEMENT

9. The organization shall ensure that information security requirements for backup and recovery management are formally defined, approved, documented, and implemented.

10. The organization shall define and approve recovery parameters, including recovery point objectives (RPO) and recovery time objectives (RTO), and ensure that backup and recovery arrangements for critical technology and information assets are designed, implemented, and periodically tested to meet these objectives.

11. The organization shall ensure that backup media, storage and facility are adequately secured and protected. Organization should perform risk assessment of the backup and restore process; and define, implement and document appropriate controls.

12. Regularly testing the restoration process should be conducted in line with the defined RTO/RPO. The integrity checks should be performed for assurance purpose.

13. The organization should devise a mechanism for continuous monitoring and evaluation of backup/restore activities. Regular audits should include this process for better visibility of effectiveness of this process to the senior management.

F. VULNERABILITY AND PATCH MANAGEMENT

14. Vulnerabilities and patch management life cycle shall be defined, documented, approved and implemented.

15. Vulnerability management shall include regular vulnerability assessments, classification of vulnerabilities based on criticality level, and effective patch management.

16. The organization shall implement a comprehensive patch management program including vulnerability testing before deployment, continuous monitoring, and a defined rollback strategy.

PKCERT

Safeguarding Pakistan's Cyberspace

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