National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2026

Essential Data Center and Web Hosting Services Controls

NTISB

A. INTRODUCTION

Pakistan Information Security Framework: **"Essential Data Center and Web Hosting Services Controls"**, outlines the baseline of information security data center controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

This framework applies to data centers, email and all hosting services, encompassing physical infrastructure, IT systems, and communication platforms used to store, process, or transmit data.

B. DATA CENTER

1. The data center's security framework shall implement comprehensive physical controls, including but not limited to controlled physical access, perimeter protection, video surveillance, visitor management, and other necessary safeguards.

2. Organizations that provide hosting services to other entities, or that maintain their own data centers or servers, shall implement and maintain the following minimum security controls:

   a) Implement network and perimeter security controls, including Next generation firewalls (NGFWs), WAFs, IDS/IPS, DDoS protection, DLP solutions, network segmentation, DMZs, and use of secure communication protocols.

   b) Implement server hardening practices including limiting unnecessary services, disabling unused ports, enforcement of secure configuration, configuration baseline management and enforcing secure protocols.

   c) Implement and maintain a documented patch and vulnerability management process to identify, prioritize, remediate, and track vulnerabilities, supported by regular vulnerability assessments and remediation verification.

d) Develop, implement, and regularly test Business Continuity and Disaster Recovery Plans to ensure operational continuity in line with organizational requirements, recovery objectives and service criticality.

e) Deploy continuous monitoring and incident response solutions, including SIEM, SOAR, and SOC.

f) Implement structured cable management practices, including labelling, separation of power and data cables, and regular inspections to prevent operational and security risks.

g) Secure logging and monitoring practices, including retention of critical security event logs for a minimum of 12 months, ensuring integrity, availability, and audit traceability.

h) Secure backup and recovery mechanisms, including encryption, access controls, periodic restoration testing, and offsite or geographically separate backup storage.

3. Data centers shall undergo regular internal audits and at least one independent annual third-party audit, covering physical, technical, and operational security controls.

4. Organizations that are unable to meet the defined audit and compliance requirements shall ensure migration of services to a secure and compliant data center that meets the requirements of this framework and applicable regulatory obligations.

5. All data centers shall strictly comply with all relevant and applicable security requirements defined in the nCERT Essential Framework, including Asset and Risk Management, System and Communication Protection, Data Protection, Identity and Access

Management, Incident Response and audit. Compliance with these requirements shall be mandatory and subject to verification and audit.

C. EMAIL AND WEB HOSTING SERVICES

6. Organizations providing email and hosting services to other government organizations or maintaining email or any other hosting services for their own users, shall define, document, approve, and implement information security requirements to ensure the confidentiality, integrity and availability of the hosted services.

7. The information security requirements for the email service shall include at the least the following:

a) Advanced email threat protection controls to detect and block phishing, malware, spam, and malicious content.

b) Implement multi-factor authentication for administrative, remote and webmail access.

c) Ensure email archiving, backup and restoration capabilities to support operational continuity and regulatory compliance.

d) Monitoring, detection, and response mechanisms to protect against Advanced Persistent Threats (APTs) and targeted attacks.

e) Email domain validation and authentication controls, including Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication Reporting and Conformance (DMARC) or equivalent measures.

D. WEB APPLICATION SECURITY

8. Organizations shall define, document, approve, and implement information security requirements for all internal and externally accessible web applications, regardless of the hosting environment (on-premises, in the cloud or third-party service providers)

9. The information security requirements for web applications shall include at least the following:

a) Controls to prevent unauthorized access, abuse and malicious activity.

b) Secure architectural and design principles with defense-in-depth protection.

c) Secure communication protocols for data in transit.

d) Well-defined secure usage practices and user awareness controls.

e) Regular vulnerability assessments, penetration testing, and remediation tracking.

f) Maintenance of applications using up-to-date, supported and securely configured components.

g) Strong authentication and session management mechanisms.

h) Secure software development lifecycle (SSDLC) practices, including code reviewing, security testing, and approval prior to deployment.

10. Organizations hosting their websites and applications outside Pakistan shall plan migration to data centers within Pakistan's geographical boundaries.

11. Organizations shall remain accountable to ensure that requisite security requirements are clearly defined, implemented, and monitored through contracts, Service Level Agreements (SLAs), and right-to-audit clauses with developers, hosting providers and cloud service providers.

E. ENVIRONMENTAL CONTROLS (DATA CENTERS AND HOSTING FACILITIES)

12. The organization shall implement and maintain environmental controls to protect data center facilities, systems, and equipment from environmental threats that may impact availability, integrity, or safety of operations.

13. Data centers shall be equipped with power supply resilience mechanisms, including uninterruptible power supplies (UPS), backup generators, and redundant power distribution, sufficient to meet defined availability and recovery requirements.

14. The organization shall implement environmental monitoring systems to continuously monitor temperature, humidity, power stability, and other critical environmental parameters, with automated alerts and defined response procedures for threshold breaches.

15. Data centers shall implement heating, ventilation, and air conditioning (HVAC) controls designed to maintain environmental conditions within manufacturer-recommended operating ranges and to prevent overheating, condensation, or equipment degradation.

16. The organization shall deploy fire detection and suppression systems appropriate for data center environments, including early warning smoke detection, automatic fire suppression, and safe evacuation mechanisms, with regular inspection, testing, and maintenance.

17. Data centers shall implement controls to mitigate risks from water leakage, flooding, dust, vibration, and other physical or environmental hazards, including raised flooring, leak detection systems, and appropriate facility design.

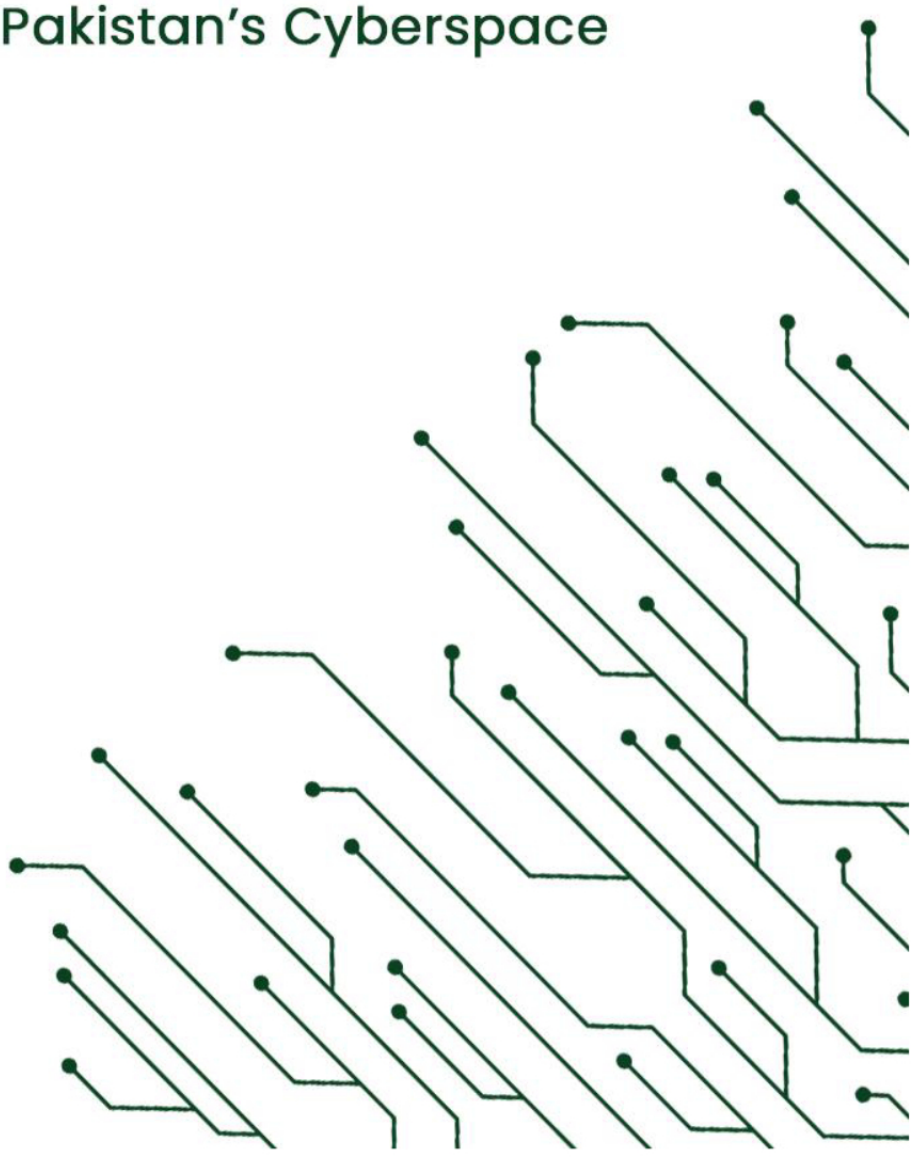
18. The organization shall document and maintain environmental control procedures, including preventive maintenance schedules, escalation processes, incident response actions, and roles and responsibilities for facility management personnel.

19. Environmental control systems and safeguards shall be periodically tested, inspected, and audited to verify effectiveness, reliability, and compliance with regulatory, contractual, and organizational requirements.

20. The organization shall ensure that environmental incidents or control failures affecting data center operations are logged, investigated, reported to relevant stakeholders, regulators, and incorporated into risk management and continuous improvement processes.

PKCERT

Safeguarding Pakistan's Cyberspace



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