PKCERT

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

Essential Data Center and Web Hosting Services Controls

NTISB

A. INTRODUCTION

Pakistan Information Security Framework 2025: **“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 encompass robust physical security measures, including access controls, perimeter fencing, video surveillance, visitor management, and other necessary safeguards.

2. Organizations that provide hosting services to entities, or that maintain their own data centers or servers, shall implement and maintain security as follows.

   a) Implement network and perimeter security controls, including NGFWs, WAFs, IDS/IPS, DDoS protection, DLP, network segmentation, DMZs, and secure protocols.

   b) Implement server hardening practices including limiting unnecessary services, disabling unused ports, and enforcing secure protocols.

   c) Implement and maintain a patch and vulnerability management process to keep systems up to date, address known vulnerabilities, prioritize critical updates, and conduct regular vulnerability assessments.

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

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

f) Implement structured cable management practices, including labelling, separation of power and data cables, and regular inspections.

g) Retain critical security event logs for a minimum of 12 months and maintain audit trials.

3. Data centers shall undergo regular internal audits and at least one annual third-party audit.

4. Organizations that do not fulfill the audit requirements shall migrate their services to a secure and compliant data center.

5. Along with the above controls, all data centers shall strictly comply with all relevant and applicable security requirements defined in the nCERT Essential Framework 2025, which encompass 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 audit.

C. EMAIL AND WEB HOSTING SERVICES

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

7. The cybersecurity requirements for protecting the email service shall include at the least the following:

a) Analyze and filter email messages, including phishing emails and spam, using advanced and up-to-date email protection techniques.

b) Implement multi-factor authentication for remote and webmail access to email services.

c) Ensure email archiving and backup to support continuity and compliance.

d) Implement secure management practices and protection mechanisms to defend against Advanced Persistent Threats (APT).

e) Validate email service domains, by using 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 cybersecurity requirements for internal and externally accessible web applications, regardless of the hosting environment (on-premises, cloud or third-party services)

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

a. Protection against unauthorized access and malicious activity.

b. Secure architectural principles with layered protection.

c. Secure communication protocols for data in transit.

d. Well defined secure usage practices for users.

e. Regular assessment of applications and systems for vulnerabilities.

f. Maintenance with up-to-date and secure components.

g. Strong authentication mechanisms.

h. Secure development practices and security testing before deployment.

10. Organizations hosting their website 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 adequately addressed in contracts and Service Level Agreements (SLAs) with developers and cloud service providers.

PKCERT

Safeguarding Pakistan's Cyberspace

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