National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2026

Essential Data Protection and Privacy Controls

NTISB

A. INTRODUCTION

1. "Pakistan Information Security Framework: **"Essential Data Protection and Privacy Controls"**, outlines the baseline of information security data protection and privacy controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

2. This framework applies to all employees, contractors, consultants, third-party service providers, and any other individuals or entities that process or access the organization's data. It covers all forms of data, including electronic, paper-based, structured, and unstructured information, regardless of where it is stored or processed. It also applies to all business functions, systems, applications, networks, and processes that involve personal, sensitive, or confidential data, whether processed within the organization's premises, in cloud environments, or through third-party arrangements.

B. DATA PRIVACY

3. The organization shall establish and maintain a clear privacy governance structure with defined roles, responsibilities, and accountability for data protection.

4. The organization shall collect and process personal data only where a lawful basis exists under applicable data protection laws, including consent where required. Privacy notices, wherever applicable, shall clearly inform data subjects of the purpose, legal basis, and use of their personal data.

5. Privacy Impact Assessments shall be conducted for new systems, projects, or processes to identify and mitigate potential privacy risks.

6. Organization shall develop and implement data privacy policy while keeping the principles of purpose limitation, data minimization, accuracy, storage limitation, maintaining confidentiality, integrity and accountability.

7. The organization shall ensure that access to personal data is monitored, logged, and auditable.

8. Organizations shall establish and maintain a documented data retention schedule. An illustrative retention schedule template is provided in Table 1, as an example, to support consistent classification, retention, and disposal of data in accordance with legal, regulatory, and business requirements.

Table 1: Data Retention Schedule Table (Example)

Data Category	**Data Description**	**Data Owner**	**Legal/ Regulatory Basis**	**Retention Trigger**	**Retention Period**	**Storage Location**	**Disposal Method**
Personal Data	Employee Record	To be defined	To be defined	End of employment	To be defined	HR system	Secure deletion
Financial Data				Fiscal year closure			
Operational Data				Creation date			
Customers data				End of contract			

C. DATA SECURITY

9. All organizational data shall be classified according to sensitivity, criticality, and regulatory requirements to ensure appropriate protection.

10. Personal and organizational data shall be collected, processed, handled, transmitted, and stored only in accordance with defined security procedures and legal requirements.

11. Access to data shall be granted strictly on the principle of least privilege and role-based access, with regular reviews and monitoring.

12. Data classified as critical or highly critical with respect to confidentiality, where the unauthorized disclosure could cause catastrophic or serious impact, shall be encrypted during transmission and preferably during storage.

13. The organization shall implement measures to maintain the accuracy, completeness, and consistency of data throughout its lifecycle.

14. Data shall be retained only for as long as necessary to fulfill business or legal purposes and shall be securely and permanently disposed of when no longer required.

15. Data shall be regularly backed up and recovery mechanisms shall be tested to ensure business continuity, in case of data loss, based on the classification of data.

16. Data access, processing, and security events shall be continuously monitored and logged to detect, prevent, and investigate unauthorized activities.

D. DATA BREACH

17. All systems and networks shall be continuously monitored to detect potential data breaches or anomalous activities at the earliest possible stage.

18. Upon detection of a breach, immediate containment measures shall be applied to limit impact and prevent further compromise.

19. The organization shall ensure timely reporting of data breaches (72 hours for critical infrastructure and 120 hours for non-critical infrastructure) to concerned regulator and nCERT.

20. Appropriate policy and procedure should be preferably developed to notify affected individuals of the breaches about compromise of their personal data, including details of risks and recommended protective measures.

21. When required, public statements regarding breaches should be issued in a controlled and coordinated manner to ensure accuracy and maintain trust.

PKCERT

Safeguarding Pakistan's Cyberspace

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