NCA-40.082025 – National CERT Advisory – Mandatory Data Protection Measures for Organizations Handling PII

Introduction

In light of increasing data breaches, identity theft incidents, and large-scale privacy violations targeting both public and private sector organizations, the National Cyber Emergency Response Team (National CERT) of Pakistan issues this advisory for all entities collecting, processing, storing, or transmitting Personally Identifiable Information (PII) of Pakistani citizens.

The National Cyber Security Policy – 2021 (NCSP-2021) mandates safeguarding the confidentiality, integrity, and availability of citizens' personal data as a matter of national security and public trust. Given the growing sophistication of cybercriminals, the widespread exploitation of misconfigured systems, and negligent data handling practices, urgent remediation measures are required to prevent financial, operational, and reputational harm.

Scope

This advisory applies to all public and private sector entities that collect, process, store, or transmit Personally Identifiable Information (PII) of Pakistani citizens including financial services, telecommunications and internet providers, commerce and logistics, government agencies, healthcare institutions, educational entities, as well as third-party and outsourced service providers. These obligations extend uniformly across on-premises, cloud, and hybrid environments, and remain binding regardless of the scale, nature, or duration of personal data processing.

Impact

Inadequate data protection practices and the absence of strong security controls can lead to:

Risk	Details
Identity Theft and Fraud	Compromise of PII enabling fraudulent financial transactions, unauthorized account access, and impersonation.
Mass Privacy Breaches	Exposure of sensitive citizen data (e.g. CNIC, contact details, health records) leading to black-market trading of personal information.
Operational Disruption	Ransomware and data-wiping incidents causing downtime, loss of productivity, and service unavailability.
Legal and Regulatory Consequences	Heavy fines, criminal liability, and loss of licenses under PECA 2016, sectoral regulations, and contractual obligations.
Erosion of Public Trust	Breaches in government, healthcare, or financial data undermining citizen confidence and damaging organizational reputation.
National Security Risks	Exploitation of aggregated citizen data for espionage, disinformation, or destabilization campaigns.

Attack Vectors

- **Database Exploitation:** SQL injection, privilege escalation, and exploitation of unpatched vulnerabilities in systems storing PII.
- **Insider Threats:** Malicious or negligent employees leaking or misusing sensitive customer records.

- **Unsecured Data Transfers:** Transmission of unencrypted PII over public or insecure networks.
- **Third-Party Compromise:** Vendors or partners with weak security controls becoming a conduit for data breaches.
- **Phishing & Social Engineering:** Manipulating staff to gain credentials or direct access to restricted systems.
- **Cloud Misconfigurations:** Exposed storage buckets, weak API protections, and public-facing services without proper access restrictions.

Common Technical & Process Vulnerabilities

Vulnerability	Description
Unclassified Data	No sensitivity classification; all records treated equally, increasing exposure risk.
Excessive Data Collection	Gathering more personal data than required for business operations.
Plaintext PII Storage	Sensitive data stored without encryption at rest.
Weak/No Encryption in Transit	Data transmitted without strong cryptographic protocols (TLS 1.2+).
Weak Credential Storage	Passwords stored without salted hashing (e.g., bcrypt, Argon2).
Overprivileged Access	Accounts granted unnecessary access to sensitive datasets.
Missing Data Disposal Policy	No secure sanitization before data deletion or media reuse.
Outdated Systems	Legacy applications or unpatched systems hosting PII.
Weak Vendor Controls	Third-party providers lacking contractual and technical security requirements.
Absent Incident Response Plan	No documented, tested procedure for data breach handling.

Threat Actors

- **Cybercriminal Gangs:** Monetizing stolen PII via identity fraud, phishing kits, and dark web marketplaces.
- **State-Sponsored APT Groups:** Using compromised citizen data for surveillance, political manipulation, and intelligence gathering.
- **Hacktivists:** Targeting organizations for ideological reasons, often leaking sensitive records publicly.
- **Malicious Insiders:** Employees or contractors exploiting privileged access for personal gain or revenge.

Recommendations & Action Items for Organizations/ Entities

Category	Action Item	Details
	I. Data Classification & Minimization	a. Classify datasets by sensitivity (Public, Internal, Confidential, Restricted). b. Collect & store only minimum PII required for business/regulatory needs.

Immediate Mitigation Measures	**II. Access Control & Authentication**	a. Implement Role-Based Access Control (RBAC) with “least privilege” principles. b. Enforce Multi-Factor Authentication (MFA) for all privileged/admin accounts.
	III. Encryption & Secure Storage	a. Encrypt PII at rest (AES-256+) and in transit (TLS 1.2+). b. Store passwords using salted hashing (bcrypt, Argon2).
	IV. Patch Management	a. Regularly update all systems and applications handling PII. b. Apply security patches promptly to fix known vulnerabilities.
Medium-Term Measures	**I. Secure Development Lifecycle (SSDLC)**	Integrate security testing throughout software development lifecycle.
	II. Data Retention Policy	a. Retain PII only for legally required durations. b. Securely dispose of outdated records.
	III. Incident Response Readiness	a. Maintain a documented breach response plan. b. Rehearse incident response including CERT communication protocols.
	IV. Vendor Risk Management	a. Audit all third-party providers handling PII. b. Enforce contractual obligations for data protection.
Strategic Long-Term Measures	**I. Regulatory Compliance Alignment**	a. Regularly review and align practices with NCSP b. 2021, PECA 2016, and sectoral laws.
	II. Continuous Security Awareness	a. Conduct quarterly training on PII protection. b. Run phishing simulation exercises.
	III. Zero Trust Data Security	Enforce verification & authentication for all access requests to sensitive systems.
	IV. Annual Security Audits	Commission independent audits of encryption, access controls, and breach readiness.
	V. Threat Intelligence Sharing	a. Collaborate with national/sectoral CERTs. b. Share IoCs (Indicators of Compromise) and emerging threat trends.
	VI. Disaster Recovery & Business Continuity	a. Develop and maintain a Disaster Recovery Plan (DRP) with defined RTO (Recovery Time Objective) and RPO (Recovery Point Objective). b. Conduct annual disaster recovery drills to test infrastructure resilience and ensure rapid restoration of critical services. c. Maintain off-site and encrypted backups of critical PII and operational data.

Recommended Actions for Individuals (Cyber Hygiene & PII Protection)

While organizations are legally bound to safeguard citizen data, individuals also have a critical role in protecting their Personally Identifiable Information (PII). Practicing good cyber hygiene reduces the risk of identity theft, fraud, and misuse of sensitive information.

Category	Recommended Action	Details

Data Disclosure	Submit CNIC and personal documents only when absolutely necessary	Clearly state in writing (e.g., on photocopies: *"For SIM registration only – Not valid for other purposes"*) before handing over documents.
Data Minimization	Avoid oversharing personal details	Share only required information with service providers; never disclose unnecessary PII (e.g., family CNICs, addresses) unless legally mandated.
Document Protection	Safeguard physical copies	Keep CNICs, passports, and official papers in secure locations. Do not leave copies unattended at offices, shops, or unverified agents.
Digital Hygiene	Protect personal data online	Avoid posting sensitive information (e.g., CNIC, phone numbers, home address) on public websites or social media platforms.
Password & Account Security	Use strong, unique passwords with MFA	Do not reuse passwords across banking, email, or social media accounts. Enable two-factor authentication wherever available.
Device Security	Keep devices updated & secured	Regularly update software, use antivirus, and avoid downloading apps from untrusted sources. Always lock devices with PIN/biometric security.
Phishing & Scams	Be alert to suspicious links or calls	Never share OTPs, banking details, or CNIC numbers over phone/email unless verified. Report suspicious activity immediately to relevant authorities.
Public Wi-Fi Use	Avoid transmitting sensitive data over free Wi-Fi	Use a VPN when accessing personal accounts on public networks.
Data Disposal	Destroy old copies of documents securely	Shred paper records; wipe digital copies before selling or disposing of devices.
Malicious Apps	Beware of downloading from unauthentic sources	Malicious apps may leak your personal data. Only install apps from trusted, verified sources like official app stores.

Reporting and Contact

Organizations experiencing or suspecting data breaches, unauthorized PII access, or related incidents are urged to:

Email: cert@pkcert.gov.pk

Web Portal: https://pkcert.gov.pk/report-incident.asp

When reporting, please include:

- Incident description and timeline
- Affected systems and data categories
- Indicators of compromise (IoCs)
- Mitigation steps already taken

Call to Action for Organizations / Enterprises

The National CERT strongly advises:

- Immediate review and remediation of all systems handling PII.
- Enforcement of encryption, access control, and data minimization as operational priorities.
- Mandatory security training for all employees and contractors.
- Continuous monitoring for unauthorized access or anomalous data activity.

Call to Action for Individuals

- Submit CNIC and personal documents only when absolutely necessary, and label copies clearly with intended use.
- Use strong, unique passwords for each account and enable multi-factor authentication.
- Avoid sharing unnecessary personal information with service providers or on social media.
- Download apps only from official app stores to prevent data leaks via malicious software.

Proactive protection of citizen data is not just a compliance requirement — it is a strategic imperative to preserve national security, protect public trust, and ensure organizational resilience.

PKCERT