GOVERNMENT OF PAKISTAN
NCERT
******

No.F.NO.1-1/2025/DG (NCERT)/ 241 **Islamabad, the 15th May , 2025**

From

Dr Haider Abbas
DG -(nCERT)

To

1- ADG (Immigration), FIA, Islamabad
2- Cabinet Secretary, CAB, Islamabad
3- Chairman, NTCOMM, Islamabad
4- Chief (Water Resources), PC, Islamabad
5- DD-Finance, API, Islamabad
6- DGPR, AGPR, Islamabad
7- DS EXP (Privatization/Overseas/IPC), MOF, Islamabad
8- DS EXP (Religious Affair/NFSR/BOI, MOF, Islamabad
9- Deputy Director Monitoring, FAB, Islamabad
10- Deputy Chief-I (Industries & Commerce), PC, Islamabad
11- Deputy Director Wafaqi Mohtasib, MONHS, Islamabad
12- Deputy Secretary (Heritage), NHCD, Islamabad
13- Director Admin/Housing, NPF, Islamabad
14- Director General, NACTA, Islamabad
15- Director General (Maritime), PC, Islamabad
16- Director General - Admin, NITB, Islamabad
17- Director General FIA, FIA, Islamabad
18- Director Procurement ERRA, NDMA, Islamabad
19- Economic Adviser, MOF, Islamabad
20- Executive DG (Admin), PEMRA, Islamabad
21- Federal Minister (Communication), MOCM, Islamabad
22- Foreign Secretary, MOFA, Islamabad
23- GM (Human Resource), PPMC, Islamabad
24- Joint Executive Director III (Liquefied Petroleum Gas), OGRA, Islamabad
25- Joint Secretary (Privatization), MOEPWD, Islamabad
26- Parliamentary Secretary, MOC, Islamabad
27- SAPM for Industries & Production Division, MOIP, Islamabad
28- Secretary, NSD, Islamabad
29- Secretary, SENATE, Islamabad
30- Secretary (Revenue Analysis), FBR, Islamabad
31- Secretary Climate Change, MOCC, Islamabad
32- Secretary ECP, ECP, Islamabad
33- Secretary Establishment Division, ESTAB, Islamabad
34- Secretary General(National Assembly), NAS, Islamabad
35- Secretary IT, MoIT, Islamabad
36- Secretary Kashmir Affair,Gilgit Baltistan & SAFRON, kagbsafron, slamabad
37- Secretary LAW & Justice, MOLJ, Islamabad
38- Secretary NTISB, CAB, Islamabad
39- Secretary Planning, PC, Islamabad
40- Secretary Railway Board, MOR, Islamabad

41- Secretary Revenue Div/Chairman FBR, FBR, Islamabad
42- Secretary Science and Technology, MOST, Islamabad
43- Secretary of Interior, MOINC, Islamabad

SUBJECT: URGENT CYBERSECURITY GUIDLINES SOCIAL MEDIA ACCOUNT MANAGEMENT

In the light of the prevailing security situation, all ministries and their attached departments are hereby advised to implement following measures forthwith to secure their official social media accounts: -

a. Reset Passwords: All official social media account passwords be reset, replacing with strong and secure credentials. Furthermore Two-Factor Authentication (2FA) be enabled with official accounts to further strengthen security.

b. Use of Official Email Accounts: Only official, designated email addresses should be used for registering and operating official social media handles.

c. Use of Personal SIMs/Emails: The practice of using personal SIM cards or personal email addresses for official social media accounts is discouraged and should be discontinued instantly. Instead, use of corporate SIMs and official designated email addresses exclusively for their intended purposes is recommended.

2. Adherence to these security measures by all will strengthen our security posture and help to mitigate cyber security risks.

Muhammad Asif
Audit Officer (Coord)
Thursday, 29 May, 2025, 10:37:54 AM

Muhammad Asif
Audit Officer (Coord)
26 May , 2025, 12:30:15 PM

Muhammad Asif
Audit Officer (Coord)
Thursday, 29 May, 2025, 10:37:54 AM

Dr Haider Abbas
DG -(nCERT)

Priority

GOVERNMENT OF PAKISTAN
NCERT
******

No.F.NO.1-1/2025/DG (NCERT)/244 **Islamabad, the 16th May , 2025**

From

Dr Haider Abbas
DG -(nCERT)

To

1- ADG (Immigration), FIA, Islamabad
2- Cabinet Secretary, CAB, Islamabad
3- Chairman, NTCOMM, Islamabad
4- Chief (Water Resources), PC, Islamabad
5- DD-Finance, API, Islamabad
6- DGPR, AGPR, Islamabad
7- DS EXP (Privatization/Overseas/IPC), MOF, Islamabad
8- DS EXP (Religious Affair/NFSR/BOI, MOF, Islamabad
9- Deputy Director Monitoring, FAB, Islamabad
10- Deputy Chief-I (Industries & Commerce), PC, Islamabad
11- Deputy Director Wafaqi Mohtasib, MONHS, Islamabad
12- Deputy Secretary (Heritage), NHCD, Islamabad
13- Director Admin/Housing, NPF, Islamabad
14- Director General, NACTA, Islamabad
15- Director General (Maritime), PC, Islamabad
16- Director General - Admin, NITB, Islamabad
17- Director General FIA, FIA, Islamabad
18- Director Procurement ERRA, NDMA, Islamabad
19- Executive DG (Admin), PEMRA, Islamabad
20- Federal Minister (Communication), MOCM, Islamabad
21- Foreign Secretary, MOFA, Islamabad
22- GM (Human Resource), PPMC, Islamabad
23- Joint Executive D rector III (Liquefied Petroleum Gas), OGRA, Islamabad
24- Joint Secretary (Privatization), MOEPWD, Islamabad
25- Parliamentary Secretary, MOC, Islamabad
26- SAPM for Industries & Production Division, MOIP, Islamabad
27- Secretary, SENATE, Islamabad
28- Secretary, NSD, Islamabad
29- Secretary (Revenue Analysis), FBR, Islamabad
30- Secretary Climate Change, MOCC, Islamabad
31- Secretary ECP, ECP, Islamabad
32- Secretary Establishment Division, ESTAB, Islamabad
33- Secretary Genera (National Assembly), NAS, Islamabad
34- Secretary IT, MoIT, Islamabad
35- Secretary Kashmir Affair,Gilgit Baltistan & SAFRON, kagbsafron, Islamabad
36- Secretary LAW & Justice, MOLJ, Islamabad
37- Secretary NTISB, CAB, Islamabad
38- Secretary Planning, PC, Islamabad
39- Secretary Railway Board, MOR, Islamabad

40- Secretary Revenue Div/Chairman FBR, FBR, Islamabad
41- Secretary Science and Technology, MOST, Islamabad
42- Secretary of Interior, MOINC, Islamabad

SUBJECT: URGENT CYBERSECURITY ADVISORY BASELINE SECURITY MEASURES FOR WEB APPLICATIONS

The National Cyber Emergency Response Team (National CERT) has issued a Cybersecurity Advisory titled **"NCA-29 (a).051625 – National CERT Advisory – Baseline Security Measures for Web Applications"** (Annexure), to establish baseline security controls for the secure development, deployment, and maintenance of web applications across public and private sectors.

2. This advisory is issued in light of persistent cyber threats exploiting common web vulnerabilities, the increasing use of third-party components, and the critical need to safeguard the Confidentiality, Integrity, and Availability (CIA) of web-facing systems. It outlines essential security practices for system custodians, developers, DevOps engineers, administrators, and third-party service providers

3. It is requested that the attached Advisory be disseminated on priority to all departments, teams, and associated service providers to take immediate action.

Annexure: NCA-29 (a).051625 – National CERT Advisory – Baseline Security Measures for Web Applications.

Dr Haider Abbas
DG -(nCERT)

Copy for information to:-

1- Director C3, NCERT, Islamabad
2- DS-NTISE, CAB, Islamabad

Dr Haider Abbas
DG -(nCERT)

National Cyber Emergency Response Team

Government of Pakistan

PKCERT

F.No.1-1/2025/DG (nCERT)/244 **Dated, the 16th May, 2025.**

Subject: **URGENT CYBERSECURITY ADVISORY – BASELINE SECURITY MEASURES FOR WEB APPLICATIONS**

The National Cyber Emergency Response Team (National CERT) has issued a Cybersecurity Advisory titled **"NCA-29 (a).051625 – National CERT Advisory – Baseline Security Measures for Web Applications"** (Annexure), to establish baseline security controls for the secure development, deployment, and maintenance of web applications across public and private sectors.

2. This advisory is issued in light of persistent cyber threats exploiting common web vulnerabilities, the increasing use of third-party components, and the critical need to safeguard the Confidentiality, Integrity, and Availability (CIA) of web-facing systems. It outlines essential security practices for system custodians, developers, DevOps engineers, administrators, and third-party service providers

3. It is requested that the attached Advisory be disseminated on priority to all departments, teams, and associated service providers to take immediate action.

Annexure: NCA-29 (a).051625 – National CERT Advisory – Baseline Security Measures for Web Applications.

(Dr. Haider Abbas, TI)
Director General
National CERT
Ph: 051-9203422

All Secretaries of Ministries/ Divisions of the Federal Government and Chief Secretaries of the Provinc al Governments

Annexure

NCA-29 (a).051625 – National CERT Advisory – Baseline Security Measures for Web Applications

Introduction

The National CERT issues this advisory to establish baseline security measures for the secure development, deployment, and maintenance of web applications. These guidelines are applicable to government organizations, critical infrastructure providers, and private organizations hosting public-facing or internal web services.

These advisory underscores the importance of protecting the Confidentiality, Integrity, and Availability (CIA) of web-based systems in light of persistent cyber threats, exploitation of web vulnerabilities, and the rising use of third-party components.

The measures outlined herein are designed for implementation by cybersecurity teams, system custodians, developers, network administrators, DevOps engineers, and third-party service providers

Impact

Failure to implement robust web application security practices may result in:

1. **Unauthorized Access** – Exploitation of unpatched components or weak authentication mechanisms.
2. **Data Breach** – Exposure or exfiltration of personally identifiable or sensitive information.
3. **Defacement and Denial of Service** – Loss of website availability or integrity due to injection or misconfiguration.
4. **Malware Injection** – Use of compromised web services to serve malware or redirect to malicious domains.
5. **Compliance Violation** – Non-adherence to national and international standards leading to legal liabilities.
6. **Reputational Damage** – Public loss of trust due to website compromise or misuse of hosted content.

Threat Details

Cyber attackers commonly exploit insecure web applications using the following Tactics, Techniques, and Procedures (TTPs):

Technique	Description
SQL Injection (SQLi)	Unauthorized query execution to retrieve or manipulate databases.
Cross-Site Scripting (XSS)	Execution of malicious scripts in users' browsers via unvalidated input.
Insecure Authentication	Use of weak passwords, lack of MFA, and session hijacking.
Unpatched TPCs	Integration of vulnerable third-party libraries or APIs.
Misconfigured Servers	Default credentials, exposed admin interfaces, and excessive permissions.

Affected Systems

- Public and internal government web portals
- Corporate web applications handling sensitive data
- APIs and backend services exposed to external users
- Systems integrated with unverified third-party components
- Applications lacking secure deployment pipelines or code audits

Recommendations & Mitigation Actions

1. Secure Web Application Development

Security by Design

- Incorporate security in SDLC from the initiation phase with risk and privacy impact assessments.
- Perform threat modeling during the design stage to identify and mitigate risks like XSS, CSRF, and SQLi.

Secure Coding Practices

- Adhere to OWASP secure coding standards.
- Use input validation via whitelisting.
- Encode all user-generated content to prevent XSS.
- Implement parameterized queries to defend against SQLi

Authentication and Session Management

- Enforce Multi-Factor Authentication (MFA) for sensitive systems and privileged users.
- Set strong password policies (minimum 14 characters, special characters required).
- Store passwords using strong hashing (e.g., bcrypt, PBKDF2).
- Ensure session security via HTTP Only and Secure cookies; implement idle timeout and session regeneration post-authentication.

Logging & Monitoring

- Log all user and administrative activity.
- Store logs securely on a **SIEM or centralized log server** for a **minimum of one year.**

2. Secure Hosting Practices

Server Configuration & Hardening

- Disable unnecessary services (e.g., FTP, Telnet); apply timely OS patches.
- Restrict administrative access to whitelisted IPs only.
- Enforce SSH/TLS for secure remote access.

Backup & Recovery

- Encrypt all backups; store them in geographically diverse locations.
- Conduct annual recovery drills to validate backup integrity.

Hosting Platform Requirements

- Select platforms compliant with national security and uptime standards.
- Implement high-availability and disaster recovery (DR) capabilities.

Incident Response Readiness

- Prepare to **immediately isolate** affected systems in case of compromise.
- Notify National CERT and internal SOC teams on confirmed incidents.
- Use trusted backups for restoration and patch root-cause vulnerabilities.

3. Perimeter & Network Defense

Firewall & IDPS Configuration

- Use a default DENY-ALL policy and allow only explicitly required traffic.
- Deploy Intrusion Detection and Prevention Systems (IDPS) to log and mitigate anomalous behavior.

Network Segmentation

- Host web servers in a DMZ; isolate from internal or admin networks.
- Position Web Application Firewalls (WAF) and Web Proxies in front of public-facing services.
- Secure administrative terminals with MFA and network segmentation.

Malware Protection & Monitoring

- Enable malware scanning for all uploaded files.
- Review logs regularly for port scans, brute-force attempts, or unusual access patterns.

4. Database Security

Access Control & Encryption

- Grant least-privilege access to applications and users.
- Prevent public exposure of database servers.
- Require MFA for DB admins; only allow access from trusted web servers.

- Use TLS 1.3 or higher for encryption in transit; encrypt sensitive data at rest.

Audit Trails & Patching

- Enable row-level auditing for sensitive tables.
- Apply vendor-released patches immediately upon availability.

Data Management

- Enforce data minimization and retention policies.
- Implement pseudonymization to de-link personal identifiers from datasets.

5. Securing Web Content

Content Publishing Governance

- Formalize approval workflows for all published material.
- Regularly audit web content for compliance with policies and legal standards.

Active Content Handling

- Store scripts in non-executable directories.
- Strictly sanitize all user-generated inputs, including file uploads.

Monitoring & Detection

SIEM Integration

- Feed logs from firewalls, applications, servers, and DBs into centralized SIEM.
- Configure alerts for unusual behaviors (e.g., failed logins, privilege escalation, unexpected queries).

Vulnerability Management

- Conduct Vulnerability Assessment and Penetration Testing (VAPT) at least twice a year.
- Maintain a formal vulnerability management program for risk remediation.

Code Quality Checks

- Use Static and Dynamic Application Security Testing (SAST/DAST) tools.
- Perform manual secure code reviews for critical systems.

Incident Response & Compliance

Preparedness

- Maintain an up-to-date **incident response plan** aligned with PKCERT escalation paths.
- Conduct red team/blue team exercises simulating web app exploitation.

Policy Compliance

- Align development and hosting with **organizational SLAs**, **NDAs**, and **legal obligations**.
- Ensure **security documentation and training** is regularly updated.

Call to Action

The National CERT strongly urges all government organizations and enterprises to:

- Immediately assess their web applications against these baseline controls.
- Implement missing safeguards and validate existing controls via testing.
- Report any suspected breaches or vulnerabilities to cert@pkcert.gov.pk.
- Collaborate with PKCERT for audits, training, or guidance related to web security.

Adhering to these baseline security measures fosters a resilient and secure digital environment, protecting organizational assets and public trust. Continuous improvement, proactive monitoring, and cross-sector collaboration are vital to guard against evolving cyber threats.