

Karachi, Dated: September 2026

To

1. The Chairman, Enquires, Anti-Corruption, Establishment of Sindh, Karachi.
2. The Chairman, Planning & Development Board, Govt. of Sindh, Karachi
3. The Chairman Sindh HEC Karachi.
4. The Senior Member Board of Revenue (BOR) Sindh, Karachi.
5. The Additional Chief Secretary, Govt of Sindh _____
6. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
7. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
8. The Administrative Secretary, Government of Sindh (All) _____
9. The Provincial Ombudsman, Sindh.
10. The Inspector General of Police Sindh, Karachi
11. The Divisional Commissioner (All) in Sindh _____

SUBJECT: STRENGTHENING THE PROTECTION AND CYBER RESILIENCE OF CRITICAL INFORMATION INFRASTRUCTURE (CII)

National Cyber Emergency Response Team (National CERT) is mandated to coordinate and strengthen cybersecurity measures across Pakistan's digital ecosystem, including the protection and resilience of Critical Information Infrastructure (CII). Considering the evolving cyber threat landscape and increasing risks to critical infrastructure from sophisticated cyberattacks, ransomware, supply-chain compromises, Advanced Persistent Threats (APTs), and other malicious cyber activities, all CII entities are hereby advised to maintain a heightened state of cybersecurity preparedness and ensure implementation of appropriate preventive, detective, responsive, and recovery measures.

2. All the CII entities are advised to undertake the following measures on priority:

a. Cyber Security Governance : Establish a dedicated cyber Security function under the leadership of a designated Chief Information Security officer (CISO) with clearly defined roles responsibilities and accountability, inventory of all critical IT/UT assets, systems, applications, databases, networks, services, a dependencies supporting essential operations.

b. Risk and Vulnerability Assessment: Conduct periodic cybersecurity risk assessments, vulnerability assessments, penetration testing, and configuration reviews of critical systems. Critical and high-risk vulnerabilities shall be remediated on priority.

c. Network Segmentation: Ensure appropriate segregation of critical IT and Operational Technology (OT) networks from general-purpose corporate networks and the public Internet. Access between network zones shall be strictly controlled, monitored, and based on operational necessity.

d. Identity and Access Management: Implement strong access controls based on the principles of least privilege and need to know. Multifactor Authentication (MFA) shall be enforced for privileged , administrative remote and other critical access.

e. Security Monitoring and Detection: Ensure centralized security logging and continuous monitoring of critical infrastructure through appropriate SIEM/SOC capabilities. Security logs shall be adequately retained to support threat detection, incident investigation, and digital forensics.

f. Endpoint and Server Security: Deploy and maintain appropriate endpoint protection, EDR/XDR, anti-malware, application control, secure configuration baselines, and timely security patching across critical systems.

g. Incident Response Preparedness: Establish and regularly test Cyber Incident Response Plans, clearly defining escalation mechanisms, roles and responsibilities, containment procedures, and coordination protocols with National CERT.

h. Business Continuity and Disaster Recovery: Maintain and periodically test Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) to ensure continuity and timely restoration of critical services following a cyber incident or disruption.

j. Backup and Recovery: Maintain secure encrypted) offline/immutable backups of critical systems and data. Backup restoration procedures shall be periodically tested to verify their integrity and effectiveness.

j. Third-Party and Supply-Chain Security Assess and continuously manage cybersecurity risks associated with vendors, contractors, service providers, cloud platforms, and other third parties having access to critical systems or sensitive information

k. Threat Intelligence and Information Sharing: Establish mechanisms for timely consumption and operationalization of cybersecurity advisories, alerts, Indicators of Compromise (IoCs), and threat intelligence issued or shared by National CERT

l. Cybersecurity Awareness and Capacity Building: Conduct regular cybersecurity awareness and specialized technical training for employees, system administrators, security teams, and senior management, with particular emphasis on phishing, social engineering, credential security, and incident reporting.

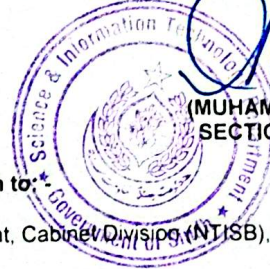
m. Compliance and Security Audits: Ensure compliance with applicable national cybersecurity policies, frameworks, standards, directives, and guidelines issued by the Government of Pakistan and National CERT, including implementation of relevant controls under the Pakistan Information Security Framework (PISF) and applicable CII protection requirements.

n. Cyber Incident Reporting: Any cybersecurity incident affecting or potentially affecting critical infrastructure, essential services, sensitive information, or national interests shall be immediately reported to National CERT through the designated incident reporting mechanism to facilitate timely coordination, technical assistance, and national-level response.

o. The management of all CII entities is requested to accord the highest priority to cybersecurity and operational resilience and ensure that cybersecurity risks are regularly reviewed at the senior management/Board level. Appropriate human, technical, and financial resources shall be allocated for the protection of critical infrastructure

p. All CII entities are further advised to conduct an immediate review of their existing cybersecurity posture against the above requirements and address identified and action taken, which may sought by National CERT as and when required

3. National CERT remains available for coordination, technical guidance, incident response support and cyber security advisories to strengthen the collective resilience of Pakistan's Critical Information Infrastructures.



(MUHAMMAD AKBAR KHAN)
SECTION OFFICER (TECH) 1/09/2026

A copy is forwarded for information and necessary action to:

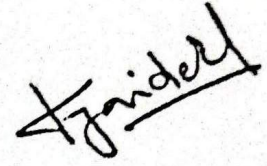
1. AS(Staff) to Chief Minister Sindh, Karachi.
2. The Assistant Secretary (NTISB), Cabinet Secretariat, Cabinet Division (NTISB), GoP.
3. PS to Chief Secretary, Sindh.
4. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
5. Staff Officer to S&IT Department, Govt. of Sindh, Karachi.
6. Webmaster, for uploading the advisory on url: <https://www.sindh.gov.pk/notifications>

SECTION OFFICER (TECH)

- inventory of all critical IT/OT assets, systems, applications, databases, networks, services, and dependencies supporting essential operations.
- c. **Risk and Vulnerability Assessment:** Conduct periodic cybersecurity risk assessments, vulnerability assessments, penetration testing, and configuration reviews of critical systems. Critical and high-risk vulnerabilities shall be remediated on priority.
 - d. **Network Segmentation:** Ensure appropriate segregation of critical IT and Operational Technology (OT) networks from general-purpose corporate networks and the public Internet. Access between network zones shall be strictly controlled, monitored, and based on operational necessity.
 - e. **Identity and Access Management:** Implement strong access controls based on the principles of least privilege and need-to-know. Multi-Factor Authentication (MFA) shall be enforced for privileged, administrative, remote, and other critical access.
 - f. **Security Monitoring and Detection:** Ensure centralized security logging and continuous monitoring of critical infrastructure through appropriate SIEM/SOC capabilities. Security logs shall be adequately retained to support threat detection, incident investigation, and digital forensics.
 - g. **Endpoint and Server Security:** Deploy and maintain appropriate endpoint protection, EDR/XDR, anti-malware, application control, secure configuration baselines, and timely security patching across critical systems.
 - h. **Incident Response Preparedness:** Establish and regularly test Cyber Incident Response Plans, clearly defining escalation mechanisms, roles and responsibilities, containment procedures, and coordination protocols with National CERT.
 - i. **Business Continuity and Disaster Recovery:** Maintain and periodically test Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) to ensure continuity and timely restoration of critical services following a cyber incident or disruption.
 - j. **Backup and Recovery:** Maintain secure, encrypted, offline/immutable backups of critical systems and data. Backup restoration procedures shall be periodically tested to verify their integrity and effectiveness.
 - k. **Third-Party and Supply-Chain Security:** Assess and continuously manage cybersecurity risks associated with vendors, contractors, service providers, cloud platforms, and other third parties having access to critical systems or sensitive information.
 - l. **Threat Intelligence and Information Sharing:** Establish mechanisms for timely consumption and operationalization of cybersecurity advisories, alerts, Indicators of Compromise (IoCs), and threat intelligence issued or shared by National CERT.
 - m. **Cybersecurity Awareness and Capacity Building:** Conduct regular cybersecurity awareness and specialized technical training for employees, system administrators, security teams, and senior management, with particular emphasis on phishing, social engineering, credential security, and incident reporting.
 - n. **Compliance and Security Audits:** Ensure compliance with applicable national cybersecurity policies, frameworks, standards, directives, and guidelines issued by the Government of Pakistan and National CERT, including implementation of relevant controls under the Pakistan Information Security Framework (PISF) and applicable CII protection requirements.
 - o. **Cyber Incident Reporting:** Any cybersecurity incident affecting or potentially affecting critical infrastructure, essential services, sensitive information, or national interests shall be immediately reported to National CERT through the designated incident reporting mechanism to facilitate timely coordination, technical assistance, and national-level response.
 - p. The management of all CII entities is requested to accord the **highest priority to cybersecurity and operational resilience** and ensure that cybersecurity risks are regularly reviewed at the senior management/Board level. Appropriate human, technical, and financial resources shall be allocated for the protection of critical infrastructure.
 - q. All CII entities are further advised to conduct an **immediate review of their existing cybersecurity posture** against the above requirements and address identified

and actions taken, which may be sought by National CERT as and when required.

3. National CERT remains available for coordination, technical guidance, incident response support, and cybersecurity advisories to strengthen the collective resilience of Pakistan's Critical Information Infrastructures.

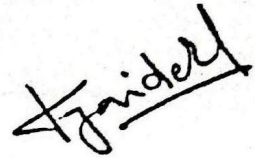
1067


Dr Haider Abbas
DG -(nCERT)
Ph:051-9203422

Copy for information to:-

- 1- Director CERT, NCERT, Islamabad
- 2- Director Cybersecurity & Privacy, MoIT, Islamabad
- 3- Secretary NTISB, CAB, Islamabad
- 4- Director GRC, NCERT, Islamabad

Dr Haider Abbas
DG -(nCERT)
30 July, 2026, 10:27:48 AM



Dr Haider Abbas
DG -(nCERT)
Ph:051-9203422