Subject: **Cyber Security Advisory - Prevention against Cyber-Attacks on the Event of National Days (Advisory No. 18)**

It has generally been observed that hostile elements tend to sabotage National Days of Pakistan by disrupting IT services of critical information infrastructure (CII), Government Ministries and departments. On the occasion of Independence Day (14 August, 2024), IT/OT services disruption attempts by hostile elements cannot be ruled out.

2. In addition, hostile elements/state sponsored malicious actors typically target IT infrastructure/websites of Defence sector and sensitive installations to tarnish the 'global' image of Pakistan.

3. It is likely that hostile elements may launch cyberattacks on CII on National Days (14 Aug and 6 Sep 2024).

4. Above in view, Cyber Security best practices are attached (**Annex-A**) to sensitize CII regulators, stakeholders, IT/website administrators and service providers to take additional security precautions (such as sustenance of internet backhaul against DDoS attack, web server hardening, traffic/integrity monitoring etc.) to avoid possible service disruption, website defacement and hacking attempts.

Annex-A

CYBER SECURITY BEST PRACTICES FOR PROTECTION OF IT INFRASTRUCTURE

Guidelines for IT/Web Admins

1. Upgrade OS and webservers to latest version.
2. Website admin panel should only be Accessible via white-listed IPs.
3. Defend the website against SQL injection attacks by using input validation technique.
4. Complete analysis and penetration testing of application be carried out to identify potential threats.
5. Complete website be deployed on inland servers including database and web infrastructure.
6. HTTPS protocol be used for communication between client web server.
7. Application and database be installed on different machines with proper security hardening.
8. Sensitive data be stored in encrypted form with no direct public access.
9. DB user privileges be minimized and limited access be granted inside programming code.
10. Proper security hardening of endpoints and servers be performed and no unnecessary ports and applications be used.
11. Updated Antivirus tools/ Firewalls be used on both endpoints and servers to
    safeguard from potential threats.
12. Enforce a strong password policy.
13. Remote management services like RDP and SSH must be disabled in production environment.
14. Deploy Web Application Firewalls (WAF) for protection against web attacks.
15. Employ secure coding practices such as parameterized queries, proper input sanitization and validation to remove malicious scripts.
16. Keep system and network devices up-to-date.
17. Log retention policy must be devised for at least 3x months on separate device for attacker's reconnaissance.

Guidelines for Email Security

1. **Use Strong Passwords**

   a. To ensure email security, always use strong passwords by employing combination of alphanumeric, Special characters, upper and lower case letter.

   b. Avoid using general and easily guessable passwords e.g. DOB, own/family names, vehicle registration number etc.

   c. Regularly change passwords.

2. **Avoid Email ID Exposure**

   a. Avoid sharing email ID with unknown persons.

   b. Always confirm the identity of the individual to/ from whom email is being sent/received.

   c. Avoid providing personal details in suspicious internet campaigns.

   d. Never use official email for private communication. Always use separate email IDs for personal and official correspondence.

   e. Never configure/ use official email on mobile phones.

3. **Be Aware of Phishing Attacks**

   a. Never open email attachments from unknown sources/senders.

   b. If an email seems suspicious, just ignore it; even don't try to unsubscribe it by clicking unsubscribe link as it may allow hacker to access your emails data.

   c. Never open any attachment without anti-virus scan.

   d. If any suspicious email is received immediately consult IT Administrator of your, organization.

4. **Always Send Password Protected Documents**

   a. All email attachments sent must be encrypted with password.

   b. Password must be communicated through a separate channel such as SMS, Call or WhatsApp message.

   c. Delete password from the sending channel (SMS, WhatsApp etc) once received by the receiving party.

5. **Use Two Factor Authentication**

a. In addition to strong passwords, also use two factor authentication e.g. OTP via call/ message, password reenter mechanism-etc.

b. Never share your One Time Password (0TP) with anyone.

6. **Use Well Reputed and Licensed Anti-Virus**

a. Endpoint (computer system or laptop) on which official email/data is being accessed/sent must be secured through reputed, licensed and updated antivirus/anti-malware solution.

b. Always keep system Firewalls activated and updated.

7. **Use Robust Paid Anti-Spam Filters**

a. Use reputed Spam Filters.

b. Do not rely on Google/Yahoo's Spam Filters as email attackers have become much sophisticated.

8. **Avoid Storing Data on Cloud Storage**

a. Never Store personal and official data on cloud storage.

b. Avoid using online document converting tools (Word to PDF etc) with cloud based data storage technology.

9. **Guidelines for Social Media Platforms, GSM and PDF Scanner**. Few guidelines (but not limited to) are as under:

a. Do not share official documents via WhatsApp, Telegram, Messenger and other so called end-to-end encrypted messaging apps/secret chatting applications as their servers are hosted outside Pakistan.

b. Do not use online PDF Scanner apps., Only scan secret documents via official hardened scanners.

c. Do not discuss secret official matters on call/SMS/landline/GSM WhatsApp etc. Use officially dedicated communication numbers.

d. Never store secret official documents in personal mobiles, PC.

e. Do not store secret official documents in online systems. Always delete data after usage.

f. Avoid using free and lucrative apps as majority of them steal data from PC and mobile phones.

g. Do not use cracked versions of software. Always install paid software from official support and store.

h. Ensure hardening of all online and offline official system.

10. **General Guidelines**

a. Public WiFi is more susceptible to attack as compared to private WiFi.

b. Public WiFi Administrator might be monitoring network traffic and data sent online via internet packets.

c. Passwords may be stored by network Administrator. Therefore, avoid using public WiFi for accessing personal/ official email.

d. Regularly check and apply security updates.

****