Subject: - **Cyber Security Advisory Secure Email Communications (Advisory No. 54)**

Recently, it has been observed that hostile intelligence agencies (HIAs) have launched new sophisticated social engineering/phishing email techniques to target key civil and military officials both inland and abroad. The malicious emails appear legitimate as they contain name and appointment of genuine office-holder from civil Govt and military setups. Resultantly, the users are honey-trapped. Furthermore, non-adherence to best cyber security/secure email practices by the end users is also contributing towards the same. Numerous potential exploits such as weak passwords, unencrypted confidential correspondence sharing with vendors and sharing of classified documents through social media apps (WhatsApp etc). Use of insecure means and media to share documents is also prone to man-in-the-middle cyber-attacks and interception by HIAs.

2. Above in view, it is emphasized that all email correspondence must be made through secure email services/internet. Officials of Govt and Military setups be sensitized to avoid sharing and seeking sensitive information through insecure media or internet from private vendors. In this regard, few essential guidelines for secure email communications are attached at **Annex-I** for compliance.

Annex-I

1. **Introduction**. Communication service is an important part of IT infrastructure within an organization. Though it is difficult to operate without requisite communication means as the same services may fall victim to hostile elements if related security practices like password protection on documents, use of encryption techniques, antispam and anti-phishing mechanism etc are not applied. It is recommended to follow secure communication practices proposed at para-2 to safeguard against hostile intrusions and sensitive data leakage.

2. **Recommendation for Email Security**

   a. **Use Strong Passwords**

      (1) To ensure phone security, always use strong passwords by employing combination of alphanumeric, special characters, upper- and lower-case letters.

(2) Avoid using general and easily guessable passwords e.g. date of births, own/family names, vehicle registration numbers etc.

(3) Regularly change password.

b. **Avoid Email ID Exposure**

(1) Avoid sharing email ID with unknown persons.

(2) Always confirm the identity of the individual to/from whom email is being sent/received

(3) Avoid providing personal details in suspicious internet campaigns.

(4) Never use official email for private communication. Always use separate email IDs for personal and official correspondence.

(5) Never configure/use official email on mobile phones.

c. **Be Aware of Phishing Attacks**

(1) Never open any attachments from unknown sources/senders.

(2) 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 email data.

(3) Never open any attachment without anti-virus scan.

(4) If any suspicious email is received, immediately consult IT Administrator of your organization.

d. **Always Send Password Protected Documents**

(1) All email attachments must be encrypted with password.

(2) Password must be communicated through a separate channel such as SMS, call or WhatsApp message.

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

e. **Use two Factor Authentication**

(1) In addition to strong password, also use two factor authentications e.g. OTP via call/message, password re-enter mechanism etc.

(2) Never share your one-time password (OTP) with anyone.

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

(1) 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.

(2) Always keep system firewall activated and updated.

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

(1) Use reputed spam filters.

(2) Do not rely on Google's/Yahoo's spam filters as email attackers have become much sophisticated.

h. **Avoid storing data on Cloud Storage**

(1) Never Store personal and official data on cloud storage.

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

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

(1) 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.

(2) Do not use online PDF scanner apps. Only scan secret documents via official hardened scanners.

* * * * *