Subject: - **Advisory - Cyber Security for National Integrated Dashboard (NID) being Developed by Ministry of Planning Development & Special Initiatives and Pakistan Bureau of statistics (PBS) (Advisory No.50)**

It has been learnt that **Ministry of Planning, Development and Special Initiatives/Pakistan Bureau of Statistics** is developing a National Integrated Dashboard (**NID**) to facilitate country's top executives in decision making. NID consists of **processed data** of many critical stakeholders such as Ministry of Finance, Ministry of Power & Energy, SBP and FBR etc.

2. In prevalent cyber environment, **cyber attacks and data compromise cannot be ruled out**. It is therefore, requested that Ministry of Planning, Development & Special Initiatives/Pakistan Bureau of Statistics to perform 3rd party cyber audit of NID prior to its deployment.

3. Moreover, correspondence related to Ministries/Divisions departments should be made using secure media. Officials of **Ministry of Planning, Development and Special Initiatives/Pakistan Bureau of Statistics** may be sensitized to avoid sharing of sensitive information through insecure media. Guidelines for secure communications are attached at **Appendix-I** for compliance, please.

4. Forwarded for information/necessary action.

Appendix-I

GUIDELINES FOR EMAIL SECURITY

1. **Introduction.** Email service (e.g., Yahoo, Gmail or an organization's own email server) is an important part of IT infrastructure. Though it is difficult to operate without operational email service, but, email service may fall victim to hostile elements if pertinent security practices like password protection on documents, use of encryption techniques, antispam and anti-phishing mechanism etc are not applied. Therefore, it is recommended to follow secure email practices proposed at **para 2 & 3** to safeguard against hostile intrusions and sensitive data leakage.

2. **Recommendations for Email Users**

   a. **Use Strong Passwords**

      (1) To ensure email 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. DOB, own/family names, vehicle registration number etc.

      (3) **Regularly change** passwords.

   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 email 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 emails 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 sent 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 passwords, also use two factor authentications e.g. **OTP** via call/message, **password reenter** 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 **Firewalls activated** and **updated**.

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

(1) Use reputed Spam Filters.

(2) Do not rely on Google/Yahoo's **Spam Filters** as email attackers have become much sophisticate.

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

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

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

i. **General Guidelines**

(1) **Public WiFi** is **more susceptible** to attack as compared to private WiFi.

(2) Public WiFi **Administrator** might be **monitoring network traffic** and **data sent online** via internet packets.

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

(4) Periodically **review email account security settings**.

(5) Regularly check and apply security **updates**.

3. Recommendations for Email Server Administrators. Following recommendations must be followed by email server administrator: -

a. **Use of Secure SSL Certificates**

(1) Email server should be hosted on secure domains with valid HTTPS SSL certificate.

(2) SSL certificate can eb obtained from trusted vendors like GoDaddy, GlobalSign or Verisign etc.

(3) Free SSL certificates may also be obtained via certificates authorities like LetsEncrypt (letsencrypt.org) or ZeroSSL etc.

b. **Prevention against Spamming, Spoofing and Phishing**. To restrict Spamming, Spoofing and Phishing, following steps must be implemented on email server (DNS record):-

(1) Sender Policy Framework (SPF)

(2) DomainKeys Identified Mail (DKIM)

(3) DMARC (Domain-based Message Authentication, Reporting and Conformance)

c. Always verify and test the domain for above configuration (**Para 3b**) by checking through online websites like **dmarcian.com** (DMARC Inspector), **dkimvalidator.com** (DKIM Validator) and **mail-tester.com** (Spam Test).

d. If email server doesn't qualify the above test (**Para 3c**) then it shouldn't be deployed in production environment.

e. **General Guidelines**

(1) Regularly examine email server configurations to prevent configuration drift.

(2) Educate and train users on use of Advanced Encryption Standard (AES) for documents (Word, PDF, PowerPoint etc) to be shared through email.

<><><>