Subject:- **Personal Cybersecurity Guidance for Government Officials (Advisory No. 41)**

A document containing cyber security guidelines from Google reiterating social-engineering aspects and mitigation measures are as under:

a. **Personal Mobile Phones**

(1) Don’t bring smartphone to meeting where most confidential or critical conversation or meeting is happening.

(2) Disable Bluetooth when not in use; don’t pair unknown devices.

(3) Be Judicious while connecting Public WiFi networks, try to connect with networks which are secure and are personally under your control.

(4) Ensure usage of strong password; use password manager (if exists) to generate random, unique and strong password generation.

(5) Ensure that device auto lock policy is applied after 10 consecutive failed password attempts and automatically lock after 5 minutes.

(6) Avoid software or hardware modifications such as Jailbreaking or rooting.

(7) Install applications from trusted source.

(8) Plan a contingency plan in case of loss or theft e.g. Activation of mobile tracking feature “Find My Mobile" and backup storage place (Alternative Digital Device/Cloud) for your data.

(9) Do not print official documents from home printers or share those on public media/applications or conduct sensitive meetings from home.

b. **Personal Machines and Networks**

(1) Upgrade to latest Operating System/Web Browser and keep it updated.

(2) Use Multi-Factor Authentication whenever possible; most online services provide an option of MFA.

(3) Leverage security software that provides layered defense via Antivirus, Anti-Phishing, Anti-Malware, Safe Browsing and Firewalls capabilities.

(4) Disable listening devices when not in use e.g. smartphone microphones, software voice assistants, baby monitors, CCTVs, home cameras etc.

(5) Use secure networks for official and personal communications by ensuring following:

(a) Network Address Translation (NAT) protocol is enabled.

(b) Change the default Service Set Identifier (SSID).

(c) If the ISP supports IPv6, ensure the router supports IPv6.

(d) Disable Universal Plug-n-Play (UPnP).

(e) Use strong passphrases of 20 characters to secure network connecting devices.

c. **General Online Safety**

(1) **Email Security**

(a) Avoid opening attachments or links from unsolicited emails.

(b) To prevent the reuse of any compromised passwords, use different password for different accounts.

(c) Always use secure email protocols (Secure IMAP or Secure POP3).

(d) Never open emails that make unusual claims “offer too good to be true”.

(2) **Social Media**

(a) Avoid posting personal information such as home address, phone number, CNIC, place of employment and other personal information that can be used to target or harass.

(b) Limit access of your information to "friends only” and always verify any friend requests outside of social networking.

(c) Review of security policies and settings available from your social network providers quarterly or when the site’s terms of use/policy changes.

(d) Opt for not exposing personal information to search engines.

(3) **Online Payments**. When shopping online, use a virtual card, instead of sharing your actual card number with the merchant. Google creates a virtual number that is shared with merchant to process your transaction.

(4) **Online Services**. Meta (Facebook, WhatsApp, Instagram) also provides a set of security tips for government officials available on the link “https://www.facebook.com/gpa/resources/basics/security”.