Subject: **Cyber Security Advisory - Safe Usage of Wi-Fi (Advisory No. 20)**

Context. Wi-Fi connections have become inevitable part of ICT infrastructure. Being a common component in any organization/household network, security of Wi-Fi routers is pivotal in purview of prevalent Cyber Security threats. Due to exponential increase in critical known vulnerabilities, default security configurations and lack of user awareness, malicious actor can gain persistent access to network/endpoints, install malware and steal sensitive/private data. In this regards, Wi-Fi connection security threats along with prevention guidelines are mentioned in ensuing paras.

2. **Security Threats Related to Wireless Networks**. Wi-Fi routers are considered one of the least secure devices, as they are focused on functionality rather than security. As per latest research, approximately one third of the discovered critical known vulnerabilities in Wi-Fi routers are neither patched nor addressed by vendors. Furthermore, lack of expertise in securing/hardening Wi-Fi routers further degrades organization's security posture. Common threats associated with Wi-Fi routers are: -

a. **Eavesdropping**. Intercepting and listening to network traffic without authorization.

b. **Rerouting attacks**. Manipulating router updates to cause traffic to flow to un-authorized destinations.

c. **Session hijacking**. Insertion of counterfeit IP packets after session establishment via IP spoofing, sequence number prediction and alteration.

d. **Session replay attacks**. Recording/manipulating and replaying arbitrary commands to carryout unauthorized action/gain access.

e. **Masquerading**. Manipulating IP packets to forged IP addresses.

f. **Unauthorized Computer Access**. Access to directories and files made available for sharing.

g. **DoS/DDoS Attacks**. Flooding a target device with sufficient traffic to render it useless to legitimate users. Compromised Wi-Fi routers can be used as bots in launching DDoS attacks.

h. **Simple Network Management Protocol (SNMP) attacks**. SNMP attacks may result in unauthorized privileged access, DoS attacks or cause unstable behavior.

3. **Indicators of Compromised Wi-Fi Routers (User End)**

a. Router login failure.
b. Slow internet speed.
c. Browser redirects.
d. Suspicious network activity.
e. Alerts from your internet provider.
f. Increase in pop-up advertisements.
g. Ransomware messages.

4. **Wi-Fi Router Hardening Guidelines**. The recommended security measures that must be taken to secure the wireless network include: -

a. **Change Default Credentials**. Web/CLI interface of Wi-Fi router be accessible only using strong and unique passwords instead of default credentials.
b. **Strength of Security Key**. Maximum length and complexity requirements for Wi-Fi security key must be met for connectivity to network.
c. **Secure Encryption Protocol**. Strongest and secure encryption protocol WPA3 be implemented for security key encryption.
d. **SSID**. Default SSID (commonly known as Wi-Fi name/ID) be changed and hidden (no broadcast).
e. **Firmware**. Firmware be kept up to date to protect the router from common known vulnerabilities in obsolete/insecure versions (through admin page).
f. **Firewall**. Firewall feature must be enabled and properly configured.
g. **MAC Address Filtering**. To prevent unauthorized devices from connecting/attempt to connect with Wi-Fi network, MAC filtering must be enabled and configured to allow minimum possible devices.
h. **Guest networks**. Provision of guest networks be disabled.
i. **Port Forwarding**. In Wi-Fi routers, port forwarding must be disabled.

j. **ACLs**. Implement Access Control Lists (ACLs) to restrict access to the router and prevent unauthorized access.

k. **Unnecessary Services**. Disable unused services and insecure ports including but not limited to telnet, FTP and SNMP to reduce the attack surface.

l. **Remote Access**. Remote management if deemed necessary be ensured only through SSH, HTTPS and VPN.

m. **uPnP and WPS**. To protect the router from illegitimate access, uPnP (Universal Plug and Play) WPS (Wireless Protected Setup) be disabled in security settings.

n. **Physical Security**. Proper lock and key mechanism for safe custody and restriction from un-authorized access be ensured.

o. **DoS Attack Prevention**. Enable DOS/DDOS prevention in routers if available.

5. For any query or reporting malware, suspicious email attachment, cyber incident, please forward the same (without downloading) on following email addresses: -

a. falcon1947@proton.me
b. asntisb2@cabinet.gov.pk

6. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.