Subject: **Cyber Security Guidelines Work from Home (Advisory No.4)**

1. **Background.** The National Telecom & Information Technology Security Board (NTISB), working under the aegis of Cabinet Division has been mandated to ensure Telecommunication and Information Technology Security at National Level. To this end all Ministries and Departments are updated by NTISB about emerging threats in the field of Telecom and IT and necessary remedial measure are also suggested by issuing frequent advisories.

2. **Context.** As the COVID-19 pandemic continues to spread in Pakistan, many organizations (Govt / Private) have decided to work from home. Since, this **massive** and **unprecedented shifts** to distant working is being initiated in **haste** and **unprepared state**, therefore cyber criminals / activists are eyeing to capitalize this widespread panic due to **naive cyber scty practices / procedures for remote work**.

3. **Cyber Security Challenges**. Although work from home is essential requirement, yet it poses following cyber security challenges: -

a. Non availability of secure channels to communicate and exchange data. Hence, over reliance on third party OTTAs (WhatsApp, Telegram etc).

b. Accessing sensitive devices / systems (Firewalls / Servers) through personal / un-secure internet connections. Malicious actors nearby can easily intercept internet traffic and harvest confidential information.

c. Use of un-protected / un-hardened devices (systems / laptops) for official works, which can be easily compromised by cyber threat actors.

d. Overlooking basic physical security practices.

e. High chances of successful phishing attacks due to non – usage of multi-factor authentication (MFA) for remote access.

f. Sharing of sensitive data in plaintext via third party email service provider.

g. For remote access of official systems / work bench, enabling remote desktop policy on servers / systems that subsequently becomes as a vulnerable gateway to hackers.

h. Lack of cyber security training and non-compliance of best practices.

4. **Best Practices.** In current environment, following best practices are suggested while working from home.

a. **User Level**

1. Do not use internet connected Laptops / systems for sensitive official work.

2. Avoid using public Wi-Fi for accessing sensitive official devices (firewalls / servers / switches etc); Public Wi-Fi's are prone to data interception.

3. Use organization provided VPNs to securely access sensitive devices (firewalls / servers etc).

4. Update OS / all software with latest security patches.

5. Do not use personal USB drives on official systems.

6. Always share sensitive data on indigenously developed platforms (applications / emails). Data to be share in encrypted form only.

7. Use built in encryption of MS Word, MS Power Point or use miscopen source software i.e AxCrypt, trucript etc.

8. Third party video conferencing platforms (Skype, Zoom) may be avoided for sensitive meetings. If it is deemed necessary, sensitize workplace users.

9. Do not click on any link forwarded / received from unknown / untrusted senders.

10. Always follow the principle of Need to know Basis i.e. do not disclose details of sensitive official tasks to family members.

11. Do not leave laptop / system / devices unattended.

b. **Administrator Level**

1.Update all devices / software incl VPNs, network infrastructure / security devices, with the latest software patches and configurations.

2. Provide hardened devices (systems / laptops) to HR working from home.

3. provide necessary awareness trainings to sensitize HR about cyber security aspects of working from home.

4. Enable Authorization, Authentication and Auditing (AAA services) on firewalls / switches / routers for remote work. All incoming / outgoing requests to be logged and regularly monitored to check for anomalies.

5. Ensure Multi Factor Authentication (MFA) and strong passwords on all devices / connections.

6. Develop in house means of communication including email system hosted locally etc.

7. SSL certificates to be installed on indigenous deployed email systems.