

Subject: -

Cyber Security Advisory – User Level Common Oversights (Advisory No. 64)

Context: Cyber Security audit of different Ministries/Departments has
 etitive critical oversights/non-conformities, particularly following:

- a. Connectivity of internal networks with internet.
- b. Ineffective password management policy.
- c. Credentials sharing.
- d. Device control mechanism are observed.

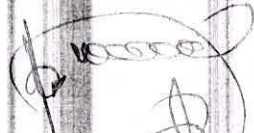
2. **Recommendations.** Following remedial measures to safeguard against falling prey to Cyber incidents are emphasized:

- a. All internal-network based IT systems/user terminals (including official correspondence system) should not be connected to internet.
- b. Password policy be enforced on all systems. Minimum criteria should include 10x character length (at least 1x special and 1x upper case character).
- c. Passwords must not be saved in browsers nor written/pasted on desks. Clear desk/clear screen policy be ensured by all appointments.
- d. Sharing of credentials (user name/password) be strictly avoided.
- e. Separate USBs (after whitelisting) be used for official systems.
- f. Strict device-control policy, particularly on USBs be implemented.
- g. Forwarding of official e-mails to personal e-mail accounts be strictly avoided.

[illegible]

FBR eDox Dy.No. 162004R
 Received in Chairman's Sec'd
 26 OCT 2023

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

A handwritten signature in dark ink, featuring a large, stylized 'S' or 'G' shape with a horizontal line through it. Below the signature, there are some initials or a second signature, possibly 'A' or 'B', also in dark ink.