राजस्थान इलेक्ट्रॉनिक्स एण्ड इन्स्ट्रूमेंट्स लिमिटेड, जयपुर

RAJASTHAN ELECTRONICS & INSTRUMENTS LIMITED, JAIPUR

[सूचना प्रौद्योगिकी विभाग /INFORMATION TECHNOLOGY DIVISION]

Subject: Cyber Security Guidelines

All concerned are requested to follow these guidelines scrupulously

1. Always use complex passwords with a minimum length of 8 characters, using a combination of capital letters, Small letters, numbers and special characters. Keep your computer locked with password. When you leave your desk temporarily, always lock/log-off from your computer session. Screen savers must have a maximum timeout period of 15 minutes or less and shall log out upon reaching the threshold and should need password to login again. Don't use the same password in multiple services/websites/apps.

2. Change your passwords at least once in 45 days or earlier. If you detect any unusual activity in your account, change the password immediately. Don't save your passwords in the browser or in any unprotected documents. Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on your table, etc.)

3. Use multi-factor authentication, wherever available.

4. Save your data and files on the secondary drive (ex: d:\). Don't save your data and files on the system drive (Ex: c:\ or root). Maintain an offline backup of your critical data. Don't upload or save any internal/restricted/confidential data or files on any non government cloud service (ex: google drive, dropbox, etc.). Don't plug-in any unauthorized external devices, including USB drives shared by any unknown person,

5. Keep your Operating System and BIOS firmware updated with the latest updates/patches. Don't use obsolete or unsupported Operating Systems.

6. Use authorized and licensed software only. Install enterprise antivirus client offered by the government on your official desktops/laptops. Ensure that the antivirus client is updated with the latest virus definitions, signatures and patches. Don't install or use any pirated software (ex: cracks, keygen, etc.). Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies, etc.).

7. Don't use any 3rd party toolbars (ex: download manager, weather tool bar, askme tool bar, etc.) in your internet browser.

8. When you leave office, ensure that your computer and printers are properly shutdown.

9. Keep your printer's software updated with the latest updates/patches.

10. Setup unique passcodes for shared printers. Don't share system passwords or printer passcode or Wi-Fi passwords with any unauthorized persons. Don't allow internet access to the printer. Don't allow printer to store its print history.

11. Download Apps from official app stores of google (for android) and apple (for iOS).

12. Before downloading an App. check the popularity of the app and read the user reviews. Observe caution before downloading any app which has a bad reputation or less user base, etc.

13. Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work. Don't use administrator account or any other account with administrative privilege for your regular work.

14. While sending any important information or document over electronic medium. Kindly encrypt the data before transmission. You can use a licensed encryption software or an Open PGP based encryption or add the files to a compressed zip and protect the zip with a password. The password for opening the protected files should be shared with the recipient through an alternative communication medium like SMS, Sandes, etc.

15. Observe caution while opening any shortened uniform resource locator (URLs) (ex: tinyurl.comlab534/). Many malwares and phishing sites abuse URL shortener services.

16. Observe caution while opening any links shared through SMS or social media, etc., where the links are preceded by exciting offers/discounts, etc., or may claim to provide details about any current affairs. Such links may lead to a phishing/ma1ware webpage, which could compromise your device. Don't open any links or attachments contained in the emails sent by any unknown sender. Don't disclose any sensitive details on social media or 3rd party messaging apps.

17. Don't use any unauthorized remote administration tools (ex: Teamviewer, Ammy admin. anydesk, etc.). Don't use any unauthorized 3rd party video conferencing or collaboration tools for conducting sensitive internal meetings and discussions. Don't use any external mobile App based scanner services (ex: Camscanner) for scanning internal documents. Don't use any external websites or cloud-based services for converting/compressing a document (ex: word to pdf or file size compression)

18. Don't use any external email services for official communication. Use only reil.co.in or gov.in or nic.in domain email ids.

19. Don't share any sensitive information with any unauthorized or unknown person over telephone or through any other medium.

20. Ensure that proper security hardening is done on the systems. Don't jailbreak or root your mobile phone. Keep the GPS, bluetooth, NFC and other sensors disabled on your computers and mobile phones. They maybe enabled only when required.

21. Report suspicious emails or any security incident to incident@cert-in.org.in and incident@nic-cert.nic.in.

22. Adhere to the security advisories published by NIC-CERT (https://nic-cert.nic.in/advisories.jsp) and CERT-In (https://www.cert-in.org.in).

*****