RAJASTHAN RAJYA VIDYUT PRASARAN NIGAM LIMITED
(AN ISO 9001-2015 CERTIFIED COMPANY)
Corporate Identity Number (CIN): U40109RJ2000SGC016485
OFFICE OF THE CHIEF ENGINEER (IT)
Vidyut Bhawan, Jyoti Nagar, Jaipur-302005

No./RVPN/SE (MIS)/XEN (MIS-I)/F.71 (20-21)(5) /D. 751 Dated: 17/2/21

General guidelines for computer system safety

Looking at the recent developments in the IT infrastructure in RVPN it is utmost necessary to follow the best practices to safeguard the systems and users from unauthorized access and other intrusions. Important guidelines for the end users for computer system safety are:

1. Users must save their data on any drive (D, E or F) other than C-Drive and make a shortcut on desktop for easy access if required.

2. Don't save any important files and data on the Desktop and as well as C-drive of computer/laptops because in case of any data corruption these files are not recoverable.

3. In case the computer system is configured with only one drive (C-Drive) then ask the system administrator for a disk partition.

4. Make backup copies of files or data you are not willing to lose on a regular basis.

5. Don't save your login information. If you browse sensitive data such as a bank account, always log out from the site. It is not enough to close the opened window or type a new address in the address bar. Many websites, especially some social networks have a feature like an automatic log on and save the username and password. If it is present, disable that option.

6. Always disable the features that store passwords. The browser has the option to store the details of every page you visit. So it is safe to disable the option. It is a simple process.

    - Open internet explorer and click TOOLS and then click INTERNET OPTIONS
    - Then click on the Content tab and click SETTINGS
    - Click to clear the checkbox for USERNAMES ON PASSWORDS AND FORMS

7. Delete your browsing history. When you leave a public computer, it is safe to delete the history of the pages visited. For this, open Internet Explorer, click TOOLS and then INTERNET OPTIONS. Delete all history, typed in address and cookies.

8. Protect the system from spyware by installing licensed Antivirus (No to Free Antivirus). Spyware or malware records personal data and sends it to a programmer or another third party which can later be used for illegal purpose.

9. Always update the Antivirus software. If there is no antivirus available then activate the windows defender firewall, which is inbuilt software available with windows operating software.

10. Make sure that there must be single antivirus software installed on the computer system. If there is more than one Antivirus installed, the system works very slowly, therefore immediately removing the old/free/de-licensed Antivirus from the system.

11. Do not respond emails from unknown persons. If you accidentally open such emails, close it immediately and change the password. The password must be strong with characters, numerals, and alphabets.

12. Take precautions while downloading any new software.

13. Don't forget to logout while using any social networks. Erase your tracks.

14. Take precautions on searching out any website on Google and click on the URL as it may direct to any untrusted URL.

15. Always keep Keyboard and mouse clean (Dust free) of the computer system.

(K.K.Meena)
Addl. Chief Engineer (IT) &
Chief Information Security Officer (CISO)
RVPN, Jaipur