रक्षा लेखा नियंत्रक का कार्यालय, गुवाहाटी उदयन विहार, नारंगी, गुवाहाटी-781171
OFFICE OF THE CONTROLLER OF DEFENCE ACCOUNTS
UDAYAN VIHAR, NARANGI, GUWAHATI: 781171.
ई-मेल/e-mail:cda-guw@.nic.in फैक्स/FAX:0361-2640204 फोन/Ph: 0361-2640394, 2641142.

IMPORTANT CIRCULAR-81

(Through website only)

Subject: Preventive measures for strengthening of Cyber Security at user end

This office has received information that there is an increased threat of compromise of the cyber assets of the department from external sources. In this regard the competent authority has directed that necessary measures be adopted to ensure the security of IT & Software assets in use/maintained by the various offices under this organization.

In this context the following instructions/advisories are appended below for strict compliance:

1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work-area at the end of the day and when they are expected to be gone for extended periods of time.
2. Desktops, Laptops should be locked when leaving the work station for breaks or other activities. Never leave the workstation unattended or with screen on. Always lock the PC when leaving the workplace.
3. Passwords may not be left on sticky notes posted on or under a computer, nor they may be written down in an accessible location.
4. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.
5. Disable Remote Desktop Connections on PC's which are connected to the internet
6. Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls. Keep your browsers upto date.
7. Perform regular backup of all critical information to limit the impact of data or system loss. Ideally this data should be kept on a separate device, and backups should be stored offline.
8. Refrain from using pendrives or other USB enabled devices
9. Do not open attachments in unsolicitated e-mails even if they come from people in your contact list, and never click on a url contained in an unsolicitated email, even if the link seems benign. In case of genuine URL's close the email and go to the organizations website directly through the browser.

10. Application whitelisting/Strict implementation of Software Restriction Policies(SRP) to block binaries running from %APPDATA% and %TEMP% path. Ransomware samples drop and executes generally executes from these locations.
11. Refrain from using or installing unwanted software including games, third party un-trusted application etc.
12. Never shut down your PC forcefully.
13. While visiting new or unknown websites never accept the cookie policy which is listed.
14. Always use NIC email to send or receive official data. Never use other email platforms such as Gmail, Hotmail etc.
15. Any official data should not be kept on PCs connected on internet.
16. The WAN & LAN network should not be interconnected with internet network and the PCs connected on WAN & LAN network should not be used for any internet activity.

Sd/

(Dr. K Lalbiakchhunga, IDAS)
DCDA (IT&SW)

No. CDAGUW/IT&SW/11/WAN/2020
Date-17/07/2020

Distributions:

1. All Section of MO CDA Guwahati
2. All GOs/SAOs/AOs of MO CDA Guwahati
3. All local Sub Offices under CDA Guwahati
4. PS to CDA

(M H Laskar)
Sr. Accounts Officer (IT&SW)