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.

(Through website only)

No. CDAGUW/IT&SW/11/WAN/2021 Dated:-21/12/2021

To

All the Section of MO CDA, Guwahati
All the Sub Offices under CDA, Guwahati

Subject: Cyber Compliance Checks of all PCs
Reference: HQrs Office letter No. Mech/IT&S/810/Cyber Security Policy Dated-29/07/2021

Please refer to HQrs. office letter cited under reference regarding the Cyber Compliance Checks of all PCs. In this regard competent authority has decided that a comprehensive internal cyber security check/audit of all PCs under the purview of CDA, Guwahati may be undertaken with following recommendations:

1. Use Linux Operating System (OS) in all internet facing machines.
2. PCs should be protected with multilevel password like power on password, user login password, Screen saver password etc.
3. Any software/drivers should be downloaded from authentic software vendors/OEM website only. Peer to peer networks such as torrents should not be used to download any kind of material.
4. User should not click on unwanted/unknown links.
5. User is to ensure that no official correspondence is done/stored on the internet machine.
6. All attachments are to be scanned using the security software prior opening /execution.
7. Users must be careful in social media activity where revealing personal/officials information or communicating with unknown persons should be strictly avoided.
8. Avoid data transmissions between official and personal devices via USB or any other transmitting media.
9. Users should report suspicious Cyber activity to their respective authorities as early as possible. Do not delete or tamper with evidences in case of any cyber security incidents.
10. General Security:
    - i). Keep systems up to date with latest security patches.
    - ii). Encrypt all sensitive information using up to date encryption standards.
    - iii).The backup data could be restored post formatting of the infected machine after scanning with licensed total security software.
    - iv). Don't use obsolete OS such as Windows 7 and previous versions.
    - v). Don't access illegitimate websites.

vi). Only the software required for official work/ correspondence should be permitted for Installation.

a. web browser- Mozilla Firefox, Google Chrome.
b. Document Processing- MS Office/ Libre Office/ Open Office.
c. System Security – Licensed version of total security software.
d. PDFs – Web browser/ Adobe Acrobat Reader.
e. Media Player – VLC Media Player
f. Compression/Zip software – Winrar.
g. Other Software such as attendance/ work utility software may be installed post approval from the HQrs. IT Section.

vii. Be cautious of tiny URLs.

Viii. Do not open attachments contains Macros like .docm, .pptm etc.

It is therefore requested to all concerned that a compliance report may be forwarded to this office positively by 03/01/2022 on email id **cdaguwedp.dad@hub.nic.in.**

This may please be accorded 'Top Priority'

(Sandeep Kumar Yadav, IDAS)
DCDA (IT)