कार्यालय रक्षा लेखा नियंत्रक (सेना)
Office of the Controller of Defence Accounts (Army)
बेल्वेडियर परिसर, आयुध पथ, मेरठ छावनी
Belvedere Complex, Ayudh Path, Meerut Cantt.
मेल cdaedp.dad@hub.nic.in

आज़ादी का अमृत महोत्सव

Important Circular

No. IT&S/712/Misc Date: 22.12.2021

To,

The Officer In charge
All section of main office and Sub Office

Sub: Cyber Compliance Checks of all PCs.
Ref: HQrs Office letter no. Mech/IT&S/810/Cyber Security Policy, Dated 12.15.2021 and 29.07.2021.

A copy of HQrs office above referred letter (available on CGDA WAN) is enclosed herewith for your strictly compliance.

This has the approval of Addl. CDA.

Encls: As Above.

-Sd-
Accounts Officer (IT&S)

Copy to:

IT&S-III - For uploading on website.

Astt. Accounts Officer (IT&S)

GENERAL OF DEFENCE ACCOUNTS – EDP
ULAN BATAR ROAD, PALAM, DELHI CANTT – 110010

Phone : 011-25665761-63 Fax : 011-25675030
Website : http://cgda.nic.in
Email : cgdanewdelhi@nic.in

No Mech/IT&S/810/Cyber Security Policy Dated: 15/12/2021

To
All PCsDA/CsDA/PrIFAs/IFAs/PCA(Fys)

Subject: Cyber Compliance Checks of all PCs

Reference: MoD letter no S/52787/MoD Cyber Cell/compromised System.

Please refer to the CGDA circular no 3805 uploaded on 28/07/2021 at http://cgdacircular.dad regarding Cyber Compliance Checks of all PCs.

2. In this context, it is intimated that compliance report from your office in this regard is still awaited.

3. It is requested to furnish compliance report positively by 21/12/2021.

Dosaj
15/12/21

(Anupam Dosaj)
Sr. AO (IT&S)

CONTROLLER GENERAL OF DEFENCE ACCOUNTS – IT&S
ULAN BATAR ROAD, PALAM, DELHI CANTT – 110010
Phone : 011-25665761-63 Fax : 011-25675030
Website : http://cgda.nic.in
Email : cgdanewdelhi@nic.in

No. Mech/IT&S/810/Cyber Security Policy Dated: 29/07/2021

To
All PCsDA/CsDA/PrIFAs/IFAs/PCA(Fys)

Subject : Cyber Compliance Checks of all PCs.

Competent Authority has decided that a comprehensive internal cyber security check/audit of all PCs under the purview of PCsDS/CsDA may be undertaken with the following recommendations:

Highlighted point action required from all section/ Sub offices.

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 sever password etc.
3. Any software/ drivers should be downloaded from authentic software venders/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 form the concerned IT section under CGDA.

vii. Be cautious of tiny URLs.
viii.Do not open attachments contains Macros like .docm, .pptm etc.

A compliance report may be forwarded to HQrs IT&S Wing at the earliest.

Jt CGDA(IT&S) has approved.

28/07

(Amit Kumar)

Sr.ACGDA(IT&S)