भारत सरकार रक्षा मंत्रालय
Government of India Ministry of Defence
रक्षा लेखा विभाग मुख्य कार्यालय
Defence Accounts Department Headquarters
उलानबटाररोड, पालम, दिल्ली छावनी-110010
Ulan Batar Road, Palam, Delhi Cantt – 110010
Ph- 011-25665586, 25665586589, 25665763 , Fax- 011-25675030
Email: cgdanewdelhi@nic.in
आई0टी0 एंड एस0 विंग IT&S WING

No: Mech/IT&S/810/Cyber Security Dated: 09/02/2022

URGENT

CIRCULAR

To
All PCsDA/CsDA/PCA(Fy)/PrIFA/IFA

Subject : Compliance to communication security advisory for government officials.

JS(Estt/Plg/Parl)/CISO , Ministry of Defence has issued directions to stop violations of Manual of Departmental Security Instructions(MoDSI) and National Security Policy Guidelines(NISPG). In order to curtail the leakage of classified information , guidelines are issued in the interest of communication security.

In this regard, the following guidelines should be followed by all the controllers in the interest of communication security:

1. The **Top Secret** and **Secret** Information shall be shared only in a closed network with leased line connectivity where SAG grade encryption mechanism is deployed.
2. The use of NIC email facility or Government Instant Messaging Platforms (such as CDAC's Samvad, NIC's Sandesh etc) are recommended for the communication of **Confidential** and **Restricted** information taking utmost care regarding the classification of information.
3. All controllers are advised to deploy proper firewalls and white-listing of IP addresses while using the e-Office system.
4. In the context of Video Conferencing for official purpose , Government VC solutions offered by CDAC, CDOT and NIC should be used. The meeting ID and password shall be shared only with authorized participants. Top Secret and Secret information shall not be shared during the VC.
5. Officials working from home., should use security-hardened electronic devices (such as Laptop, Desktop etc) which are connected to the office servers through a VPN and firewall setup. It is pertinent to mention that Top Secret/ Secret information shall not be shared in the 'work from environment'.
6. Digital Assistants devices like Amazon's Echo, Apple's HomePod etc. should not be kept in office. Digital Assistants (such as Alexa, Siri etc.) should be turned off in the smart phones/watches used by the officials.

7. Public messaging platforms like whatsapp, telegram etc. should not be used for any classified official communication.

8. In view of the above, all Controllers are directed to ensure strict compliance of the guidelines given above for communication security. Action taken report may please be forwarded to this office at earliest.

(Sandeep Bansal)
Sr. ACGDA(IT&S)