D.G. Systems & D.M.
Dairy No. 267
Date. 2/11/2022

Receipt no 2887132/2022/NC-II

F.No.N-24015/1/2022-CC
Government of India
Ministry of Finance
Department of Revenue

New Delhi, dated 1st October, 2022

OFFICE MEMORANDUM

Subject : Communication Security Advisory for Government Officials.

In order to curtail the leakage and misuse of classified information through public domain messaging platforms like Whatsapp, Telegram, etc., and to prevent violation of information security instructions as provided in Manual of Departmental Security Instructions (MoDSI) and National Information Security Policy Guidelines (NISPG), the following guidelines are reiterated in the interest of the communication security. All Officers/Officials of Department of Revenue are requested to follow these guidelines to ensure communication security:

1. Classified information falls under the following four categories, namely TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED. The Top Secret and Secret document shall not be shared over the internet. **According to NISPG, 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.** However, Confidential and Restricted information can be shared on internet through networks that have deployed commercial AES 256-bit encryption.
2. The use of **Government Email** (NIC email) facility or Government Instant Messaging Platforms (such as CDAC's Samvad, NIC's Sandesh, etc.) is recommended in the Ministry/Departments for the communication of Confidential and Restricted information. However utmost care should be taken during the classification of information and before the communication of the same over internet (i.e. an information which may deserve a Top Secret/Secret classification shall not be downgraded to Confidential/Restricted for the purpose of sharing the information over the internet).
3. In the context of **e-Office System**, proper firewalls may be deployed and IP addresses may be white-listed. The 'e-Office server' may be accessed through a Virtual Private Network (VPN) for enhanced security. It has to be ensured by the concerned authority that only authorized employees are allowed access to the e-Office System. However, Top secret/Secret information shall be shared over the e-Office system only with leased line closed network and SAG grade encryption mechanism.
4. In the context of **Video Conferencing** (VC) for official purpose, Government VC solutions offered by CDAC, CDOT and NIC may be used. The meeting ID and password shall be shared only with authorized participants. To ensure better security, the "Waiting Room" facility and prior registration of the participants may be used. Even then, Top Secret and Secret information shall not be shared during the VC.
5. Officials working from home, may use security-hardened electronic devices (such as Laptops, Desktops, etc.). Such devices may be connected to the office servers through VPN and Firewall setup. It is pertinent to mention that Top Secret/Secret information shall not be shared in the 'work from home' environment.