

Shram Shakti Bhawan,  
Rafi Marg, New Delhi-1  
24<sup>th</sup> January, 2022

CIRCULAR

It has been observed that a large number of Government officials were using public domain messaging platform like Whatsapp, Telegram, etc. for classified official communication. It is a clear violation of information security instructions as provided in the Manual of Departmental Security Policy Guidelines (NISPG). Classified information shared on public domain messaging platforms like Whatsapp can be harvested by private companies owning the platform, as they control storage servers that are often located outside the country, which can be used by adversaries or can be monetized for gains.

2. In order to curtail the leakage of classified information and misuse of such platforms, following guidelines are issued for the officers/officials of the department for compliance in the interest of the communication security-

a) 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.

b) Pertinently, 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 Ministries/Departments for the communication of Confidential and Restricted information. However, utmost care should be taken during the classification of information and before the communication 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).

c) In the context of **e-Office** system, the Ministry/Department may deploy proper firewalls and white-listing of IP addresses. The e-Office server accessed through a Virtual Private Network (VPN) for enhanced security. The Ministry/Department may ensure that only authorized employees are allowed to 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.

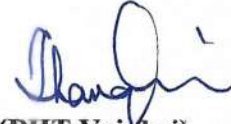
d) In the context of **Video Conferencing** (VC) for official purpose, Government VC solutions offered by CDAC, CDOT and NIC may be used. The meeting ID and password shall be shared only with authorized participants. To ensure better security, the 'Waiting Room' facility and prior registration of the participants may be used. Even then, Top Secret/ Secret information shall not be shared during the VC.

e) 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 a VPN and Firewall setup. It is pertinent to mention that Top Secret/ Secret information shall not be shared in the 'work from home' environment.

Contd:

f) Digital Assistant devices like Amazon's Echo, Apple's HomePod, Google Home, etc. may be kept in office. Further, Digital Assistants (such as Alexa, Siri, etc.) should be turned off in the smart phones/watches used by the employee. Smart phones may be deposited outside the meeting room during discussion on classified issues.

3. This issues with the approval of the Competent Authority, and treated as **TOP priority**.



**(BHT Vaiphei)**  
**Under Secretary (e-Gov)**  
**Tel.No.23766944**

Copy to –

1. All Wings/Divisions/Branches/Sections heads, DoWR, RD & GR
2. NIC, DoWR with a request for uploading on intra-mowr.