



**Government of Jammu and Kashmir**  
**General Administration Department**  
Civil Secretariat, Srinagar.

Subject: Discretion in Handling Official Communication of Sensitive/  
Secret/Confidential Nature.

**Circular No: 26 –JK(GAD) of 2024**  
**Dated: 22-11-2024**

It has come to the attention of the administration that there is an increasing trend among officers and officials to use third-party tools such as WhatsApp, Gmail, and other similar platforms for transmitting sensitive, secret, and confidential information. This practice poses significant risks to the integrity and security of the information being communicated.

Using third-party communication tools can lead to several potential issues including unauthorized access, data breaches, and leaks of confidential information. These platforms are not specifically designed to handle classified or sensitive information, and their security protocols may not meet the stringent standards required for official communications. Consequently, the use of such tools could result in severe security breaches that jeopardize the integrity of governmental operations.

To emphasize the importance of exercising discretion and adhering to established protocols for handling official communications, particularly those of a sensitive, secret, or confidential nature, the following guidelines are issued for the officers/officials of Union Territory of Jammu and Kashmir:-

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) The use of government email (NIC email) facility or government instant messaging platforms (such as CDAC's Samvad, NIC's Sandesh etc.) is strongly recommended for the communication of CONFIDENTIAL and RESTRICTED information. Care should be taken during the classification of information; information that deserves a TOP SECRET/ SECRET classification shall not be downgraded to CONFIDENTIAL/ RESTRICTED for the purpose of sharing.

c) In the context of the e-Office system, the Departments must deploy proper firewalls and white-list of IP addresses. The e-Office server should be accessed through a Virtual Private Network (VPN) for enhanced security. Departments may ensure that only authorized employees/personnel 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) Regarding Video Conferencing (VC) for official purposes, only Government VC solutions offered by CDAC, CDOT and NIC may be used. Meeting ID and passwords should only be shared with authorized participants. For enhanced security, the 'Waiting Room' facility and prior registration of the participants may be utilized. Even then, Top Secret/ Secret information shall not be shared during the VC meetings.

e) Officials working from home should use security-hardened electronic devices (such as Laptops, Desktops, etc.) connected to office servers via a VPN and Firewall setup. It is important to note that Top Secret and Secret information should not be shared in a work-from-home' environment.

f) Digital Assistant Devices such as Amazon's Echo, Apple's HomePod, Google Home, etc. should be kept out of the office during discussions on classified issues. Further Digital Assistants, (such as Alexa, Siri, etc.) should be turned off during official meetings in the office used by employee. Smart phones should be deposited outside the meeting room when discussing classified information.

In light of the potential risks outlined above, all officers and officials are directed to adhere strictly to these guidelines to ensure the security and confidentiality of official communications. Non-compliance with these directives may result in disciplinary action as deemed appropriate by the administration.

**By order of the Government of Jammu and Kashmir.**

  
(Sanjeev Verma) IAS

**Commissioner/Secretary to the Government**

No.GAD-MTG0SSB/12/2023-04-GAD

Dated: **22.11.2024**

Copy to the:-

1. Financial Commissioner (Additional Chief Secretary), Jal Shakti Department.

2. Additional Chief Secretary to the Hon'ble Chief Minister.
3. Director General of Police, J&K.
4. All Principal Secretaries to Government.
5. Principal Secretary to the Lieutenant Governor.
6. Additional Secretary (Jammu, Kashmir and Ladakh), Ministry of Home Affairs, Government of India.
7. All Commissioner/Secretaries to the Government.
8. Chief Electoral Officer, J&K.
9. Principal Resident Commissioner, J&K Government, New Delhi.
10. Divisional Commissioner, Kashmir/Jammu.
11. Chairperson, J&K Special Tribunal.
12. All Heads of the Department/ Managing Directors.
13. All Deputy Commissioners.
14. Secretary, J&K Public Service Commission.
15. Director, Archives, Archaeology and Museums, J&K.
16. Director Information, J&K.
17. Director, Estates, Kashmir/Jammu.
18. Secretary, J&K Services Selection Board.
19. General Manager, Government Press, Jammu/Srinagar.
20. Private Secretary to the Chief Secretary.
21. Private Secretary to Commissioner/Secretary to the Government, General Administration Department.
22. Incharge Website, GAD.
23. Government Order file/Stock file.