



**GOVERNMENT OF JAMMU AND KASHMIR
GENERAL ADMINISTRATION DEPARTMENT
CIVIL SECRETARIAT, J&K**

Subject:- Implementation of Standard Operating Procedure (SOP) for Secure Video Conferencing using NIC Bharat VC Platform across all Administrative Departments of J&K.

**Circular No:15-JK(GAD) of 2025
Dated:13.08.2025**

With the advent of IT and allied e-Governance modules in administration, there has been an increasing reliance on Video-conferencing for official communications and meetings as a convenient, time saving tool that enhances efficiency and promotes economy within the administrative system. The increasing use of video conferencing, however, necessitates strict adherence to established safety and security standards to ensure compliance with prescribed practices.

In the above backdrop, the Information Technology Department and the NIC has prepared a detailed Standard Operating Procedure (SOP), outlining comprehensive security protocols, access controls, content protection measures, along with an incident response mechanism aligned with cyber security directives of the Government of India.

The SOP aims to ensure that all virtual communications across departments are conducted with government-grade security compliance and is annexed as "**Annexure**" to this circular for strict implementation by all Administrative Secretaries, Heads of Departments (HoDs), Field Offices and all concerned.

**Sd/-
(M.Raju) IAS**

Commissioner/Secretary to the Government


No. GAD-ADM0III/84/2025-08-GAD

Dated:13.08.2025

Copy to:-

1. All Financial Commissioners (Additional Chief Secretaries).
2. Director General of Police, J&K.
3. All Principal Secretaries to the Government.
4. Principal Secretary to Hon'ble Lieutenant Governor, J&K.
5. All Commissioner/Secretaries to the Government.
6. Chief Electoral Officer, J&K.
7. Principal Resident Commissioner, J&K Government, New Delhi.

8. Joint Secretary (JKL), Ministry of Home Affairs, Government of India.
9. Divisional Commissioner, Kashmir/Jammu.
10. Director, J&K Institute of Management, Public Administration & Rural Development.
11. All Deputy Commissioners.
12. Director Information, J&K.
13. Chairperson, J&K Special Tribunal.
14. All Heads of the Departments/Managing Directors.
15. Secretary, J&K Public Service Commission.
16. Director, Archives, Archaeology and Museums, J&K.
17. Director Estates, Kashmir/Jammu.
18. Secretary, J&K Service Selection Board.
19. Secretary, J&K Legislative Assembly.
20. OSD/Private Secretary to Hon'ble Chief Minister, J&K.
21. SIO, NIC, J&K.
22. Private Secretary to Chief Secretary, J&K.
23. Private Secretaries to all Hon'ble Ministers, J&K.
24. Private Secretary to Advisor to Hon'ble Chief Minister, J&K.
25. Private Secretary to Commissioner/Secretary to the Government, General Administration Department.
26. Circular/Stock file/Website, GAD. **"Hindi and Urdu versions shall follow."**


13.08.2025
(Rohit Sharma) JKAS
Additional Secretary to the Government

Annexure to Circular No.15-JK(GAD) of 2025
dated:13.08.2025

1. Security Framework Overview

NIC Bharat VC Security Features:

- Robust encryption protocols for secure data transmission.
- Advanced access control mechanisms.
- On-premises solution ensuring enhanced data security.
- Password protection and meeting lock capabilities.
- Government-grade security compliance.

2. Pre-Meeting Security Protocols

2.1 Meeting Setup

Meeting Host Responsibilities:

- Generate unique meeting credentials for each conference.
- Set strong passwords (minimum 8 characters with alphanumeric and special characters).
- Enable waiting room/lobby feature when available.
- Configure appropriate security settings before scheduling.

2.2 Participant Invitation Process

One-to-One Sharing Protocol:

- Share VC links and passwords individually with each authorized participant.
- Use secure communication channels (official email, encrypted messaging).
- Avoid mass distribution or group sharing of meeting credentials.
- Maintain participant list with contact verification.

3. Meeting Credential Management

3.1 Link and Password Distribution

Secure Distribution Methods:

- Share meeting link and password through separate communications.
- Use official government email systems.
- Avoid sharing via unsecured platforms (WhatsApp, SMS, public forums).
- Implement need-to-know basis for meeting access.

3.2 Participant Responsibilities

Safeguarding Requirements:

- Do not forward or share meeting credentials with unauthorized persons.
- Delete meeting invitations after the conference concludes.
- Report any suspected security breaches immediately.
- Use official devices and networks when possible.

4. During Meeting Security Measures

4.1 Access Control

Meeting Commencement:

- Verify participant identity before granting access.
- Use waiting room feature to screen attendees.
- Lock meeting once all authorized participants have joined.
- Monitor participant list throughout the session.

4.2 Content Security

Information Protection:

- Disable recording unless specifically authorized.
- Restrict screen sharing to authorized personnel only.
- Avoid discussing classified information without proper clearance.
- Monitor for unauthorized participants or suspicious activity.

5. Post-Meeting Security Protocols

5.1 Immediate Actions

Session Closure:

- End meeting for all participants when concluded.
- Generate new credentials for recurring meetings.
- Archive meeting logs as per retention policy.
- Report any security incidents immediately.

5.2 Follow-up Measures

Documentation:

- Maintain attendance records
- Document any security concerns or breaches.
- Update participant lists for future meetings.
- Review and improve security measures based on experience.

6. Incident Response Procedures

6.1 Security Breach Protocol

Immediate Response:

- End meeting immediately if unauthorized access detected.
- Document incident details (time, participants, nature of breach).
- Report to NIC within 2 hours.
- Notify all legitimate participants of the security incident.
- Conduct security review before resuming VC activities.

6.2 Preventive Measures

- Regular security awareness training for all users.
- Periodic review of access logs and meeting records.
- Update security protocols based on emerging threats.
- Coordinate with NIC for security updates and patches.

7. Compliance and Monitoring

7.1 Departmental Responsibilities

Administrative Departments:

- Implement this SOP across all video conferencing activities.
- Designate VC security coordinators.
- Conduct regular compliance audits.
- Report quarterly security metrics to central IT authority.

7.2 User Training Requirements

Mandatory Training Components:

- Security features of NIC Bharat VC platform.
- Best practices for meeting credential management.
- Incident recognition and reporting procedures.
- Regular refresher training (quarterly).

8. Escalation Matrix

Incident Level	Response Time	Reporting Authority
Minor (Password sharing)	Immediate	Departmental ISO/CISO
Major (Unauthorized access)	Within 2 hours	NIC
Critical (Data breach)	Within 1 hour	Cyber Cell (details enclosed)

09. Review and Updates

- SOP Review Schedule: Semi-annually or as needed.
- Update Triggers: Security incidents, platform updates, policy changes.
- Approval Authority: Chief Information Officer.
- Distribution: All administrative departments and stakeholders.

10. Contact Information

- For Technical Support: NIC Help Desk.
- For Security Incidents: Cyber Cell (details enclosed).

This SOP is largely based on NIC Bharat VC Web Security Protocols (Para 97) and shall be strictly adhered to by all government departments and personnel in the UT of J&K.


13.08.2025
(Rohit Sharma) JKAS
Additional Secretary to the Government