CHANDIGARH POLICE
OFFICE OF THE DIRECTOR GENERAL OF POLICE, UT CHANDIGARH
ADDL. DELUX BUILDING, SECTOR-9, CHANDIGARH-160009

No. /UT/HAC dated Chandigarh the;

To

The Home Secretary,
Chandigarh Administration,
Chandigarh

Subject: **Standing Order No.83/2026, SOP for the Functioning of the Centre for Cyber Operations and Security (CenCOPS), Sector-18/A, Chandigarh.**

Sir,

Please refer to the subject cited above.

A copy of Standing Order No.83/2026, Standing Operating Procedure (SOP) for the Functioning of the Centre for Cyber Operations and Security (CenCOPS), is sent herewith for information and necessary action.

Sr. Superintendent of Police/Cyber Crime,
for Director General of Police,
UT, Chandigarh.

No. 10498-11536 UT/HAC dated Chandigarh the 10.09.2026

A copy is forwarded to the following for information and necessary action, to the:-

(i) All SSsP/SsP
(ii) All SDPOs/ all DSsP
(iii) All SHOs / I/C all Units
(iv) Reader to DGP/UT, IGP/UT, DIGP/UT
(v) I/C Computer Section (to upload the same on the official website of Chandigarh Police)

10.09.2026

Sr. Superintendent of Police/Cyber Crime,
for Director General of Police,
UT, Chandigarh.

STANDING ORDER
No. 83 /2026

SOP for the Functioning of the Centre for Cyber Operations and Security (CenCOPS), Sector-18/A, Chandigarh

1. Introduction

The Centre for Cyber Operations and Security (CenCOPS) has been established by Chandigarh Police as specialized cyber operations hub located at the Old Government Press Building, Sector-18/A, Chandigarh.

CenCOPS is envisioned as a Centre of excellence in the field of cybercrime prevention, detection, and digital forensics. It strengthens the cyber security posture of the Union Territory by enabling comprehensive response mechanisms to cyber threats and digital crimes, including high-tech investigations, real-time surveillance, and analytical policing.

2. Purpose and Functions

The primary functions of CenCOPS include:

- Cybercrime investigation and response
- Digital forensics and electronic evidence recovery
- Predictive policing using AI and data analytics
- Real-time monitoring of cyber threats
- Sentiment analysis and public outreach
- Facial Recognition System (FRS) integration
- Malware analysis and dark web surveillance

3. Infrastructure and Layout

CenCOPS is equipped with:

- Reception & Case Registration Desk
- Digital Forensics Laboratory
- Cybercrime Investigation Lab
- Open-Source Intelligence (OSINT) Analysis Room

- Real-Time Monitoring & Surveillance Room
- Data Analytics and Predictive Policing Wing
- Evidence Storage Room (Malkhana)
- Administrative Wing
- Training Room / Conference Hall
- Server & IT Backend Room

All areas are monitored with secure access control and equipped with high-end computing infrastructure, forensic toolkits, evidence imaging devices, and licensed software.

4. Domains of Operation

4.1 Digital Forensics

- Analysis of mobile phones, computers, CCTVs, DVRs, USBs, hard drives
- Recovery of deleted data and logs
- Extraction of evidence using forensic imaging tools
- Image/video enhancement and report generation

4.2 Predictive Policing

- AI-based crime mapping and heat zone prediction
- Use of data from CCTNS, emergency calls, and citizen complaints
- Generating alerts on repeat offences or trending threats

4.3 Cybercrime Investigation

- Handling cases of phishing, UPI frauds, fake investment apps, sextortion, etc.
- Technical analysis of social media links, email headers, IPs, domains
- Drafting notices to platforms under IT Act/CrPC

4.4 OSINT

- Tracking digital footprints from public platforms
- Identification of hate speech, viral misinformation, threats
- Mapping trends from news, social media, forums, and dark web

5. Intaking of Device

1. Request Submission: IO submits a written request for technical assistance through SHO/In-charge, SDPO/DSP Unit & SSP/SP to SP Cyber.
2. Forwarding: SP Cyber forwards the request to CenCOPS through Dy.SP Cyber with instructions.
3. **Documentation**:
    - The exhibit and letter are received and logged at CenCOPS reception.
    - Case details are entered into the Case Management System (CMS).
    - Acknowledgment is issued to the IO along with noted objectives.
4. **Tagging & Storage**:
    - Exhibits are QR-tagged for unique identification.
    - Stored in the Evidence Malkhana under lock and surveillance.
5. **Assignment**:
    - The Admin/In-charge assigns the case to a qualified digital forensic expert.
6. **Evidence Handling**:
    - Evidence log maintained during check-in/check-out from Malkhana.
    - Chain-of-custody strictly documented.
7. **Examination**:
    - Expert performs analysis as per case objectives.
    - Preliminary findings are recorded.
8. **Reporting**:
    - Reports uploaded to CMS; copy handed to IO.
    - Note included: "For investigative purposes only – not court-admissible".
9. **Confidentiality & Data Security**:
    - No unauthorized access to forensic labs or case files.
    - CCTV surveillance and visitor logs maintained.

6. Roles and Responsibilities

6.1 SP Cyber

- Overall supervision of CenCOPS functioning.
- Approval and forwarding of technical examination requests.

6.2 Dy.SP Cyber

- Supervises daily operations.

- Ensures proper routing of requests and communication between IOs and experts.
- Monitors case timelines and quality of analysis.

6.3 SHO/PS-Cyber & In-charge CenCOPS (Sub-Inspector Rank)

- Ensures round-the-clock operation of all labs and facilities.
- Maintains inventory and functioning of forensic tools and software.
- Ensures QR tagging, custody logs, and chain-of-evidence protocols.
- Manages CMS and supervises timely report submission.
- Coordinates training programs for officers and IOs.
- Ensures that every staff member signs a Non-Disclosure Agreement (NDA).

6.4 Forensic Expert / Technical Analyst

- Examines the digital exhibits as per best forensic practices.
- Maintains strict chain of custody.
- Uploads findings in CMS and flags concerns, if any.
- Respects legal boundaries (e.g. bypassing passwords only with approval).

6.5 Malkhana Officer (ASI/SI)

- Manages case reception, issue receipts, and track exhibit movement.
- Maintains visitor and evidence registers.

7. Confidentiality and Integrity

- Unauthorized access of official data is not allowed i.e. Photography of workstation Screen, copy of any systems Data or to share the data outside the proper channel.
- Not to carry mobile phones and personal storage devices in the lab.
- Logs of entry and exit of personnel are maintained.
- All external communications regarding technical findings must be approved by SP Cyber.

8. Training and Capacity Building

- CenCOPS to organize trainings for IOs and staffs of different LEAs.
- As per requirement of training module Industry Experts can be hired.
- A hands-on demo lab will be used for practical learning.
- For Training I/C CenCOPS to move proposal for approval.

9. Monitoring and Review

- SP Cyber will submit a performance report of CenCOPS to W/DGP or IGP.

10.Data Security and Internal Security

10.1 Roles and Responsibilities

Staff Role	Responsibilities
Lab Manager	Coordinates daily work, assigns cases, monitors deadlines, manages staffing, and ensures smooth workflow between sections.
Network forensics analyst (Resident Engineer/ System Admin)	Reviews network logs, packet captures, firewall records, and intrusion alerts to trace unauthorized activity.
Digital forensic Analyst	Collects, preserves, and analyses data from computers, storage devices, emails, cloud accounts, and mobile devices.
Evidence Custodian	Receives evidence, records it, labels it, stores it securely, and maintains the chain of custody from intake to release.
Incident response analyst	Responds to cyber incidents, isolates affected systems, captures volatile data, and supports containment and investigation.
Malware analyst	Studies malicious files or code, identifies behaviour, extracts indicators of compromise, and helps determine attack methods.
Lab technician / Support staff	Maintains equipment, prepares work areas, handles supplies, and assists analysts with routine tasks.

10.2 Safety Measures for Data Security

To ensure maximum data safety and maintain a safe laboratory environment, the following measures are to be followed:

- All devices received in the laboratory to be examined on an isolated forensic workstation to maintain data security, preserve evidence integrity, and prevent contamination of the main network.

- All the Systems having Forensic tools must be on Isolated Network (No Internet Access) connected and must be monitored with the SIEM.
- All the system logs and connected devices must be monitored.

For above the following initiatives should be undertaken to align with the organization's information security framework:

Security Initiative	Policy Alignment
Network Segmentation & Isolation	Micro-segmentation to minimize lateral movement and isolated forensic environments.
NAS (Network Attached Storage) Implementation & Drive Sharing	File exchange through approved secure channels (NAS) and prohibiting unapproved sharing.
Firewall Policies	Ensuring policies adhere to the principle of least privilege and prohibit "any-any" rules.
RDP (Remote Desktop Protocol) Port Management	ensuring remote access is controlled and monitored.
SIEM (Security Information & Event Management) Setup	Mandate centralized logging and real-time monitoring.
EDR (Endpoint Detection & Response) Deployment	Requiring centrally managed commercial Antivirus/EDR solutions on all endpoints.
DLP (Data Loss Prevention)	To monitor, control, and prevent unauthorized transfer of sensitive data across endpoints, networks, email, and cloud environments, thereby reducing the risk of data loss and ensuring compliance

10.3 Regular Audits

A mandatory quarterly audit schedule shall be implemented for the Cyber Lab, wherein comprehensive security assessments will be conducted every three months to evaluate security controls, identify gaps, and ensure adherence to applicable security protocols and standards.

Director General of Police,
UT, Chandigarh

10.4 Request Letter Format for Intaking of Digital Evidence

To **Through Proper Channel**

The Superintendent of Police
Cyber, UT Chandigarh.

Subject: ***Request for Technical Assistance from CenCOPS in FIR No. ___ dated ___ u/s ___, PS ___ and Complaint/DDR No. ------***

Sir,

It is submitted that investigation of case *FIR No. ___ dated ___ u/s ___, PS ___ and Complaint/DDR No. ----*. The case involves aspects that require specialized technical assistance and digital forensic analysis.

Details of Technical Assistance Required:

1. **Device(s) submitted**:
    - Mobile Phone / Laptop / DVR / Other (Specify with Make & Serial No.)
2. **Nature of Assistance Required**:
    - Data extraction/recovery
    - Deleted file recovery
    - Image/video enhancement
    - Social media/IMEI/IP analysis
    - Any other (Please specify)
3. **Specific Queries/Objectives for Examination**:
    - (List all investigation queries clearly)

The exhibit(s) have been sealed and submitted along with this request or by hand. You are kindly requested to forward this case to CenCOPS for necessary action.

Signature & particular
of Requesting Officer
Date

SHO/Insp/I/C

SDPO /DSP Unit

SSP/SP

SP/Cyber

DSP/Cyber

I/C CenCOPS