



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

STANDING ORDER No. 84/2026

Constitution, Functions and Operational Framework of the State Cyber Crime Coordination Centre (S4C), Chandigarh Police

1. Preamble

With the rapid growth of digital technologies and increasing dependence on cyberspace, cybercrime has emerged as a significant threat to public safety, financial security, governance and critical information infrastructure. Cyber offences transcend geographical boundaries and involve sophisticated techniques requiring specialised investigation, digital forensic capabilities, cyber threat intelligence and coordinated response mechanisms. The Ministry of Home Affairs, Government of India, through the Indian Cyber Crime Coordination Centre (I4C), has envisaged the establishment of State Cyber Crime Coordination Centres (S4Cs) in all States and Union Territories to strengthen cybercrime prevention, investigation, prosecution and cybersecurity at the State level.

Accordingly, the State Cyber Crime Coordination Centre (S4C), Chandigarh Police, is hereby constituted and notified vide order No.600126-HIII(2)-HIII(2)-2026/6090 dated 27.07.2026. As the apex cybercrime coordination and cybersecurity organisation of Chandigarh Police to provide strategic leadership, technical expertise and operational coordination for combating cybercrime and enhancing cyber resilience within the Union Territory of Chandigarh.

2. Objectives

The primary objectives of the S4C shall be:

- a. To establish an integrated and coordinated framework for the prevention, detection, investigation and prosecution of cybercrime.
- b. To strengthen cybersecurity within Chandigarh Police.

- c. To facilitate timely response to cyber incidents and cyber financial frauds.
- d. To develop technical capabilities through research, innovation and capacity building.
- e. To coordinate with the Indian Cyber Crime Coordination Centre (I4C), Central and State Law Enforcement Agencies, financial institutions, telecom service providers, social media intermediaries and other stakeholders.
- f. To promote cyber awareness, cyber hygiene and victim-centric services throughout the Union Territory.

3. Constitution and Administrative Control

The Centre shall be headed by an officer not below the rank of DIG/SSP, who shall function as the Head, State Cyber Crime Coordination Centre (S4C) and shall be responsible for policy formulation, strategic planning, operational supervision, inter-agency coordination and overall management of all cybercrime and cybersecurity-related activities within Chandigarh Police.

The Head of S4C shall ensure effective coordination with the Indian Cyber Crime Coordination Centre (I4C), CERT-In, Central Government Ministries, Financial Institutions, Telecom Service Providers and other stakeholders for strengthening cybercrime response and cybersecurity.

4. Organisation Structure

The State Cyber Crime Coordination Centre shall comprise specialised functional divisions dealing with cyber investigation, cyber operations, cyber security, digital investigation support, cyber intelligence, training, research, innovation and administration.

Each Functional Division shall be supervised by a Non-Gazetted Officer (NGO) deputed from Police Station Cyber Crime, Chandigarh Police. The concerned NGO shall be responsible for the administration, supervision, operational planning, monitoring, coordination, implementation of Standard Operating Procedures, maintenance of records and timely disposal of work relating to the respective Division.

The NGOs shall function under the direct supervision of the Head of S4C and shall maintain close coordination with Police Station Cyber Crime, CenCOPS, Cyber Desks,

District Police Units, Central Agencies, Financial Institutions, Telecom Service Providers, Internet Service Providers, Social Media Platforms and other stakeholders.

5. Functional Components of S4C

The operational functioning of the State Cyber Crime Coordination Centre shall be carried out through Police Station Cyber Crime and the Centre for Cyber Operations and Security (CenCOPS), Chandigarh Police.

(A) Police Station Cyber Crime

Police Station Cyber Crime shall function as the statutory law enforcement component of S4C and shall perform all policing functions relating to cybercrime including registration of FIRs, Zero e-FIRs, investigation of cybercrime cases, collection and preservation of digital evidence, arrest of accused persons, prosecution before competent Courts, execution of warrants, liaison with prosecution agencies and coordination with other Law Enforcement Agencies.

The Police Station shall coordinate with Banks, Financial Institutions, Payment Gateways, Telecom Service Providers, Cryptocurrency Exchanges and other stakeholders for preservation of electronic evidence, freezing of fraudulent transactions and recovery of proceeds of crime. It shall investigate both cyber-dependent and cyber-enabled offences in accordance with law.

(B) Centre for Cyber Operations and Security (CenCOPS)

CenCOPS shall function as the technical and operational arm of the S4C and shall provide specialised technical support to Police Station Cyber Crime, Cyber Desks and other Units of Chandigarh Police.

CenCOPS shall undertake cyber threat intelligence, cyber patrolling, digital forensics, malware analysis, Open Source Intelligence (OSINT), cyber security audits, incident response, social media monitoring, artificial intelligence-based analytics, cyber research, innovation, public awareness programmes and specialised capacity-building initiatives.

CenCOPS shall also function as the nodal technical centre for development of emerging technologies, cyber security of police digital infrastructure and coordination with I4C, CERT-In and other national technical organisations.

6. Functional Divisions

The S4C shall consist of the following Functional Divisions:

1. Cyber Investigation Division.
2. State Digital Investigation Support Centre (S-DISC).
3. State Cyber Crime Training Centre.
4. State Cyber Outreach, Research and Innovation Unit.
5. Administration Division.
6. Cyber Threat & Social Media Monitoring and Enforcement Division.
7. Emergency Response Division comprising:
 - a. National Cyber Crime Helpline (1930) Call Centre.
 - b. State Cyber Fraud Mitigation Centre (SCFMC).
 - c. Proactive Mitigation System for Online Crimes Against Women and Children.
8. Cyber Security Division.

The In-charge of each of the above Functional Divisions shall be a Non-Gazetted Officers deputed from Police Station Cyber Crime, Chandigarh Police, who shall be responsible for day-to-day supervision, coordination, reporting and operational management of the respective Division.

7. Cyber Desks

To strengthen cybercrime response at the Police Station level, Cyber Desks have been established in all jurisdictional Police Stations of Chandigarh Police.

The Cyber Desks shall function under the overall supervision of the Station House Officer (SHO) concerned and shall provide the first level response to cybercrime complaints.

The Cyber Desks shall deal with cybercrime complaints involving financial loss up to ₹50,000 (Rupees Fifty Thousand only) and shall undertake preliminary enquiry, victim assistance, coordination with banks and other stakeholders, and such action as prescribed under the Standard Operating Procedures issued from time to time.

Cases involving financial loss exceeding ₹50,000/- organised cybercrime, technically complex investigations, inter-State ramifications or other cases requiring specialised investigation shall be referred to Police Station Cyber Crime for appropriate legal action.

8. Women and Children Related Cyber Crimes

All cybercrime complaints relating to women and children, including cyber stalking, online sexual exploitation, cyber bullying, sextortion, child sexual abuse material (CSAM), image morphing, online harassment and other related offences, shall be dealt with by the Women Police Station, Chandigarh, in accordance with the applicable laws and Standard Operating Procedures, with necessary technical assistance from S4C and CenCOPS wherever required.

9. Functions and Responsibilities

The S4C shall serve as the central coordinating agency for all cybercrime-related matters within Chandigarh Police. It shall formulate policies, issue Standard Operating Procedures, monitor cybercrime trends, maintain cybercrime databases, conduct cyber threat assessments, develop investigative methodologies and facilitate inter-State and inter-agency coordination.

The S4C shall provide specialised technical assistance to all Cyber Desks, Police Stations and Investigating Officers in matters relating to digital evidence, mobile forensics, cloud investigation, cryptocurrency investigation, financial investigation, social media investigation, OSINT and cyber intelligence.

The Centre shall maintain effective coordination with the National Cyber Crime Reporting Portal (NCRP), National Cyber Crime Helpline (1930), Cyber Fraud Mitigation Centre (CFMC), Indian Cyber Crime Coordination Centre (I4C), CERT-In, financial institutions, telecom service providers, social media intermediaries and all other stakeholders for prompt preventive, investigative and emergency response.

10. Human Resource Management and Capacity Building

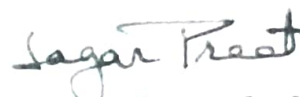
The S4C shall adopt a hybrid staffing model comprising police personnel, cyber experts, digital forensic analysts, cybersecurity specialists, legal experts, data analysts and other domain specialists.

Regular training programmes, workshops, seminars, certification courses and simulation exercises shall be organised for Police Officers, Investigating Officers, Cyber Desk personnel and technical staff to strengthen institutional capability and ensure adoption of best practices in cybercrime investigation and cybersecurity.

11. Coordination and Review

The CEO, State Cyber Crime Coordination Centre (S4C) shall conduct periodic review meetings to assess cybercrime trends, monitor investigation of important cases, review cyber security preparedness, evaluate the performance of all Functional Divisions, Police Station Cyber Crime, CenCOPS and Cyber Desks, and submit quarterly and annual performance reports.

All concerned to ensure meticulous compliance accordingly.



**Director General of Police,
UT, Chandigarh.**

No. 11912-60 /UT/HAC dated Chandigarh the 21-09-2026

A copy is forwarded to the following for taking necessary action accordingly: -

1. IGP UT
2. DIG UT
3. SSP Security & Traffic
4. SSP UT
5. All SPs
6. All SDPOs
7. All DSsP
8. All SHOs
- ✓ 9. I/C Computer Section (to upload the same on the website of Chandigarh Police.)