**Government of Jammu and Kashmir**
**Home Department**
Civil Secretariat, Jammu/Srinagar

**Government Order No. 371 (ISA) HOME of 2026**
**Dated: 17.07.2026**

**Subject: Establishment of Jammu & Kashmir Cyber Crime Coordination Centre (JK4C).**

Sanction is hereby accorded to the establishment of the Jammu & Kashmir Cyber Crime Coordination Centre (JK4C) as an independent organization under the overall superintendence and control of the Director General of Police, J&K, for coordinating, preventing, detecting and investigating cybercrimes in the Union Territory of Jammu & Kashmir.

The JK4C shall function as the nodal cybercrime coordination agency of the Union Territory of the J&K and shall align its activities with the Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs, Government of India. It shall be headed by an IGP ranked officer of the Police Department who shall be the Chief Executive Officer (CEO), JK4C.

**It is further ordered that:**

1. The subject of Cyber-Crime shall stand detached from the Crime Wing of J&K Police, and shall henceforth be dealt with by JK4C.
2. The existing 02 Zonal Cyber Crime Investigation Centres of Excellence (CICEs) established vide S.O. 232 dated 09.05.2022 and 23 District Cyber Police Stations established vide S.O. 82 dated 07.04.2025 shall form an integral part of JK4C.
3. The proposal for creation of posts of various categories required for JK4C shall be processed separately in accordance with the prescribed procedure after completion of all the requisite formalities.
4. Till the creation and regular filling of posts, the Police Headquarters, J&K shall deploy the requisite number of Police personnel of the rank of DySP and below to JK4C from the existing strength of J&K Police to ensure immediate operationalization of the Centre.

The organizational structure, tentative staff strength, operational framework and the workflow of various verticals including the functions and responsibilities of the heads of Divisions/ Units of the Jammu & Kashmir Cyber

Crime Coordination Centre (JK4C) is appended as **Annexure-A**, with this Government Order.

**By order of the Hon'ble Lieutenant Governor.**

**Sd/-**
(Chandraker Bharti) IAS
**Principal Secretary to the Government**

No. HOME-ISA/82/2021-01-HOME (CC: 23157) Dated: 17.07.2026

**Copy to the:**

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 the Hon'ble Lieutenant Governor
5. All Commissioner/Secretaries to the Government
6. Divisional Commissioner, Jammu/Kashmir
7. Inspector General of Police, Jammu/Kashmir
8. Inspector General of Police, Crime, J&K
9. All Deputy Commissioners
10. All District Senior Superintendents of Police
11. Director Information, J&K
12. Director, Archives, Archaeology & Museums, J&K.
13. Private Secretary to the Chief Secretary, J&K.
14. Private Secretary to Principal Secretary to the Government, Home Department.

**Copy also to the:**

1. Additional Secretary, JKL, Ministry of Home Affairs, GoI.
2. CEO, Indian Cyber Crime Coordination Centre (I4C).

**(Rouf Ahmad Lone) JKAS**
Under Secretary to the Government

## Annexure-A

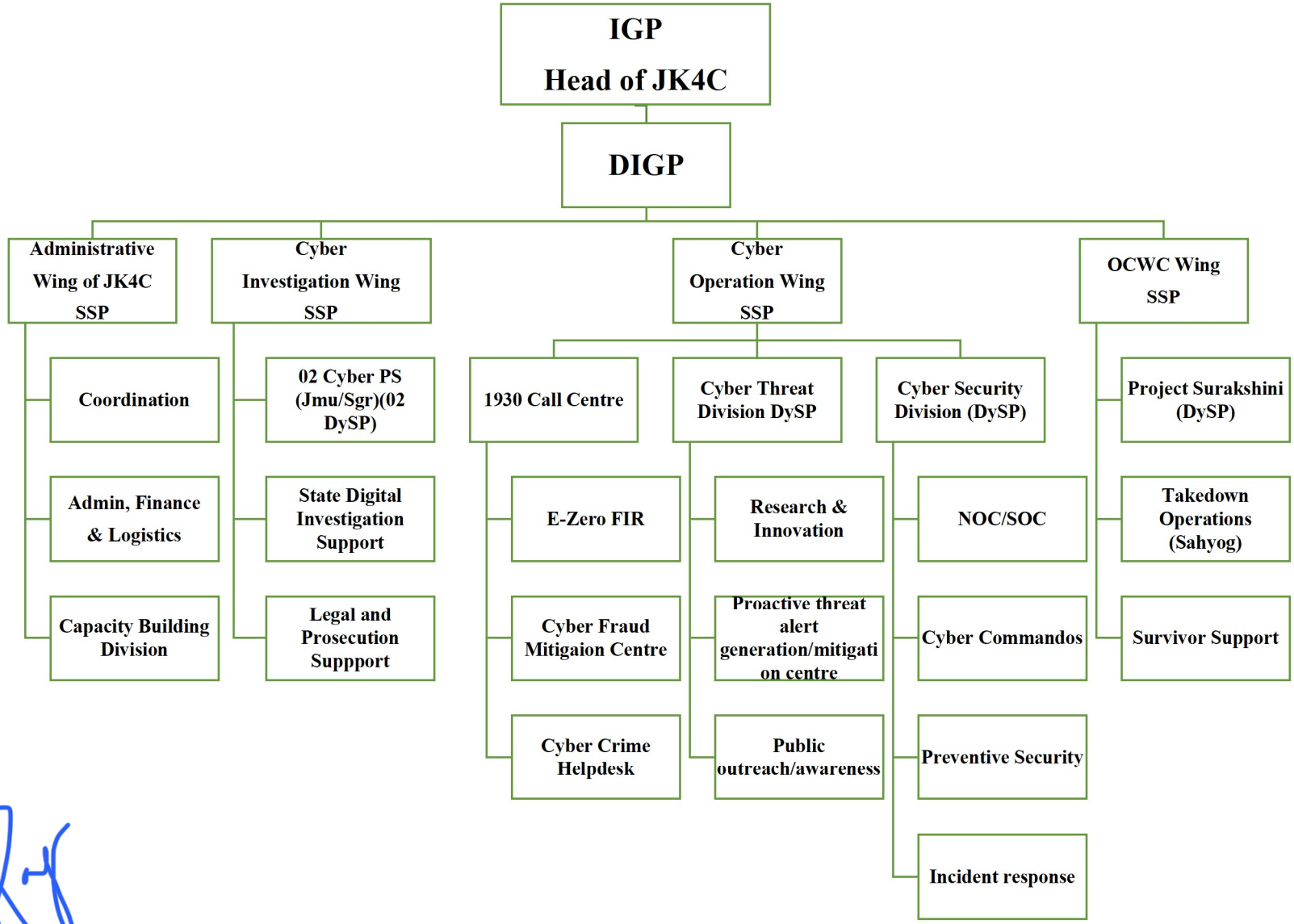
## ORGANIZATIONAL STRUCTURE

JK4C shall serve as the UT-level nodal agency to coordinate all efforts towards detection and prevention of cybercrimes in J&K and shall be headed by a dedicated IGP rank Police officer, supported by a DIGP as well as other senior officers, in a pyramidical structure, so as to ensure robust governance and strategic direction in managing cyber issues. It shall comprise specialized units, each tasked with distinct responsibilities for controlling cybercrime and strengthening cybersafety in the UT.

**JK4C shall consist of the following four Wings:**

i. Administrative Wing
ii. Cyber Investigations Wing
iii. Cyber Operations Wing
iv. Online Crimes Against Women and Children (OCWC) Wing

# ORGANIZATION CHART OF JK4C



# TENTATIVE STAFF STRENGTH

| Rank | | IG | DIG | SSP/ SP | DySP | DySP (S) | PO | Insp. | Insp (Tel) | SI | SI (Tel) | SI (S) | ASI | HC | HC/ SgCt (M) | SgCt /Ct | (AO/ AAO) | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Admin Wing JK4C HQ** | HQ | 1 | 1 | 1 | 0 | 1 | 1 | 6 | 1 | 6 | 2 | 2 | 4 | 06 | 02 | 15 | 01 | **50** |
| | Capacity Building Division | 0 | 0 | 0 | 1 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | **07** |
| **Cyber Investigation Wing** | HQ | 0 | 0 | 1 | 1 | 0 | 1 | 2 | 1 | 3 | 2 | 1 | 2 | 2 | 2 | 05 | 0 | **23** |
| | Investigation Division (Jmu/Sgr) | 0 | 0 | 0 | 2 | 0 | 2 | 10 (05 each for Jmu & Sgr) | 02 (01 each for Jmu & Sgr) | 10 (05 each for Jmu & Sgr) | 4 (02 each for Jmu & Sgr) | 0 | 12 (06 each for Jmu & Sgr) | 10 (05 each for Jmu & Sgr) | 0 | 30 (15 each for Jmu & Sgr) | 0 | **82** |
| | | 28 cyber experts for S-DISC as per Annexure –A1 | | | | | | | | | | | | | | | | |
| **Cyber Ops Wing** | HQ | 0 | 0 | 1 | 1 | 0 | 0 | 2 | 1 | 2 | 1 | 0 | 2 | 2 | 01 | 05 | 0 | **18** |
| | 1930-Call Center | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 2 | 2 | 0 | 2 | 10 | 0 | 25 | 0 | **44** |
| | Cyber Threat Division | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 2 | 2 | 0 | 0 | 0 | 0 | 6 | 0 | **12** |
| | Cyber Security Division | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 2 | 2 | 0 | 0 | 0 | 1 | 10 | 0 | **18** |
| | | 30 cyber experts as specified in Annexure –A2 | | | | | | | | | | | | | | | | |
| **OCWC Wing** | HQ | 0 | 0 | 1 | 1 | 0 | 0 | 2 | 1 | 4 | 1 | 0 | 4 | 6 | 1 | 12 | 0 | **33** |
| | | 06 counselors as per Pt. 13 in Annexure A1 | | | | | | | | | | | | | | | | |
| **Grand Total** | | **1** | **1** | **4** | **9** | **1** | **4** | **26** | **09** | **33** | **16** | **3** | **28** | **36** | **7** | **108** | **1** | **287** |

## FUNCTIONS AND RESPONSIBILITIES OF CEO, JK4C

i. The Head of JK4C shall function under the overall superintendence and control of the Director General of Police (DGP), J&K.

ii. S/he shall work in coordination with the Wing/Zone/Range/District police units and Intelligence Wing (CID), to provide support in prevention, registration and investigation of cases related to various cybercrimes.

iii. S/he shall supervise generation of intelligence and maintenance of surveillance over threat actors in accordance with the provisions of law, plan and execute special operations against cyber offenders and organized cybercriminals or gangs.

iv. S/he shall be the Nodal Officer to co-ordinate with various national level agencies, agencies dealing with cybercrimes in other States/UTs and other Government Departments in the J&K UT.

v. S/he shall commission studies and research to understand the various dimensions of cybercrimes, effect of counter measures, global trends, best practices/models in partnership with academic institutions, NGOs, private sector organizations and submit recommendations to the Government for necessary policy changes through the DG-P, J&K.

vi. S/he shall co-ordinate with IT industry and other stakeholders, both in Government and non-Government sectors, to establish linkages for research, build capacities, devise strategies for prevention of cybercrimes, improve the quality of investigation and promote cyber safety.

vii. S/he shall perform such other duties as may be assigned by the Government and DGP, J&K from time to time.

viii. S/he shall be competent to create and re-organize various subunits of JK4C J&K, based on exigencies within the sanctioned strength, with the approval of the DGP, J&K.

## WORKFLOW OF JK4C VERTICALS AND FUNCTIONS & RESPONSIBILITIES OF OFFICERS

## I. Administrative Wing (HQ) of JK4C J&K

The Administrative Wing, i.e. JK4C HQ, shall act as the strategic nerve center of the organization and oversee day-to-day operations, administrative decisions, capacity building and financial management of the JK4C HQs and its sub-units. This Wing shall be headed by an SSP rank officer who shall also function as Staff Officer (SO) to the Head of JK4C. The following Divisions shall function under this Wing:

### A. Coordination Division

i. The Coordination Division shall function as the central liaison and communication hub of the JK4C. It shall facilitate coordination with Police Headquarters, district police units, government departments, financial institutions, telecom service providers and other stakeholders involved in cybercrime prevention, investigation and cyber security operations. The Division shall act as the nodal point for coordination with Central Agencies such as MHA, 14C, NCRB, CERT-In, NPCI, etc., for information sharing, technical assistance and operational support relating to cybercrime and cybersecurity and ensure timely submission of reports and responses. Further, the Division shall monitor implementation of cyber policies, government directives, SOPs and projects undertaken by the JK4C. It shall coordinate international cooperation requests received through Interpol, MLAT channels and foreign law enforcement agencies and facilitate inter-state coordination for investigation of cybercrime cases, service of notices, execution of warrants and exchange of intelligence. The Division shall also ensure effective communication, timely response and seamless coordination among all stakeholders involved in cyber policing across Jammu & Kashmir.

ii. This Division shall also maintain regular interaction with district cyber cells and district police units. The district cyber cells shall function as the field-level extension of the JK4C. They shall provide first-response capacity for cybercrime complaints, coordinate investigations, conduct awareness programs and liaise with district administration. These units shall ensure implementation of cyber policies and operational directions issued by the JK4C. Presently, 23 Cyber PSs are working in each district of J&K UT as per SO-82 of 2025 of J&K.

### B. Administration, Finance & Logistics Division

i. The Administration, Finance & Logistics Division shall be responsible for managing the administrative, financial and logistical functions as the housekeeping hub of the JK4C. The Division shall oversee human resource management including recruitment, deployment, transfers and maintenance of service records of personnel posted within the JK4C. It shall be responsible for preparation of the annual budget, financial planning, expenditure monitoring and ensuring efficient utilization of resources.

ii. The Division shall coordinate procurement of cyber investigation tools, forensic equipment, software solutions, communication systems and other operational resources required for functioning of various wings and units of the JK4C. It shall also be responsible for vehicle management, infrastructure development and maintenance, asset and inventory management, and provision of logistical support to all units. Further, the Division shall manage contracts, service agreements and vendor relationships to ensure timely procurement, maintenance and uninterrupted availability of critical infrastructure and technical resources required for cyber policing operations across Jammu & Kashmir.

**C. Capacity Building Division**

i. The Capacity Building Division shall be responsible for developing the cyber capabilities of police personnel and allied stakeholders. Given the rapidly evolving nature of cybercrime, continuous learning and skill enhancement shall continue to remain a critical yet dynamic function. The Division shall formulate training plans, identify skill gaps and develop standards to promote professional excellence in cyber investigations and cybersecurity. This Division shall be headed by a DySP rank officer and shall function as the nodal institution for capacity building and skill development of police personnel, prosecutors and other stakeholders. The Centre shall design and conduct Basic Cybercrime Investigation Courses for newly inducted investigators and law enforcement personnel to familiarize them with cybercrime trends, legal provisions, digital evidence handling and investigation procedures.

ii. The Centre shall also conduct Advanced Investigation Courses focusing on complex cybercrime investigations, cyber financial frauds, cryptocurrency-related offences, darknet investigations and emerging cyber threats. It shall also organize Specialized training programs in Digital Forensics, Cyber Security, Malware Analysis, Open-Source Intelligence (OSINT), Cyber Threat Intelligence and Incident Response, on a regular basis. In addition, the Centre shall collaborate with national and international institutions, conduct workshops, seminars, cyber range exercises and certification programs to ensure continuous upgradation of capabilities and professional excellence within Jammu & Kashmir Police.

## II. Cyber Investigation Wing

This Wing shall be headed by an SSP rank officer, subsuming the present setup of Cyber Crime Investigation Centre for Excellence (CICE) J&K and further comprise 03 Divisions, viz:

**A. Cyber Police Stations**

i. This Division shall house two Zonal-level Cyber Crime Police Stations, one each at Jammu and Srinagar. The Cyber Crime Police Station at Jammu shall exercise jurisdiction over the Jammu Division while the Cyber Crime Police Station at Srinagar shall exercise jurisdiction over Kashmir Division. The primary mandate of these Police Stations shall be to register, investigate and prosecute cybercrime cases which are highly sensitive, spread across international borders and those which are referred to by Govt./Police Hqrs.

ii. The Division shall further ensure inter and intra state coordination for cybercrime investigations and investigation assistance.

**B. State Digital Investigation Support Centre (S-DISC)**

This Centre shall provide specialized technical assistance during cybercrime investigations. It shall maintain advanced laboratories for mobile forensics, computer forensics, cloud forensics, network forensics, CCTV examination and cryptocurrency investigations. Investigating officers from across the UT shall be able to seek assistance for extraction, preservation, examination and interpretation of digital evidence. The Centre shall also assist in expert testimony and preparation of technical reports for courts.

i. **Cyber Resource Centre-Core Unit**

The Core Unit will serve as the nerve Centre of the S-DISC, responsible for overall management, coordination and quality assurance of all specialized operations. It will house legal, administrative, and technical oversight functions. The key responsibilities include:

a. **Strategic Direction:** Led by a Centre Head/Senior Cybercrime Expert, responsible for guiding investigations, setting priorities and ensuring alignment with S-DISC directives.

b. **Operational Leadership:** Cybercrime Team Leaders and Members will coordinate investigative assignments, ensure collaboration across functional units and support district-level police with technical input.

c. **Legal Guidance:** Cyber Law Experts will provide legal vetting for investigative actions, ensure adherence to IT Act and allied legislations, and prepare legally sound documentation for prosecution.

d. **Technical Management:** System/Database Administrators and IT Specialists will manage the S-DISC hardware, software and databases, ensuring seamless, secure and uninterrupted operations.

e. **Cyber Forensics Unit**

**e.1** Collection, imaging, preservation and analysis of digital evidence from computers, storage media and TOT systems.

**e.2** Advanced malware and ransomware analysis to identify propagation mechanisms.

**e.3** Examination of compromised systems to trace intrusions and prepare forensically admissible reports.

ii. **Mobile & Smartphone Cyber Forensics Unit**

a. Data extraction and analysis from Android, iOS and other platforms.

b. Recovery of deleted messages, media and location history.

c. Reverse engineering of mobile malware and IMEI/SIM tracking support.

iii. **OSINT Unit**

a. Continuous monitoring of OSINT and social media platforms (SOCMINT) for ascertaining crime patterns, identifying threat actors,

tracking attempts at spreading misinformation, hate speech & radicalization and planned illegal activities.

b. Trend and sentiment analysis for early warning vis-à-vis potential law-and-order issues.

iv. **Dark Web & Deep Web Analysis Unit**

a. Surveillance of darknet forums and marketplaces for illegal transactions.

b. Cyber patrolling for tracking of drugs, arms, counterfeit goods and stolen data.

c. Crypto tracing of transactions linked to darknet activities.

v. **Blockchain & Cryptocurrency Analysis Unit**

a. Blockchain forensics to trace cryptocurrency-based financial crimes.

b. De-anonymization of transactions on Bitcoin, Ethereum and other blockchain platforms.

vi. **Data Aggregation & Analytics Unit**

a. Crime pattern analysis and intelligence support.

b. Tracking criminal movement, jail release patterns and inter-state cyber offender activities.

c. Build historical crime datasets and suspect profiles.

d. Integrate data from NCRP, Crime Review data, 14C, and judicial outcomes for systemic learning.

e. Prepare dashboards for strategic intervention planning and predictive policing.

f. Development of crime heat maps, offender profiles and link analysis reports.

vii. **Cyber Security Unit**

a. Act as a first responder to major cyber incidents.

b. Respond to malware attacks, ransomware, system breaches, etc.

c. Visit incident spots and collect digital artefacts for forensic analysis.

d. Conduct triage, analyses logs, and trace root causes of cyber incidents.

e. Issue technical guidelines to departments and coordinate with CyMac for major breaches.

f. Vulnerability scanning, penetration testing and remediation for government networks.

viii. **Cyber Threat Analysis Lab**

a. Identifying and neutralizing threats in the cyber domain such as malware, ransomware, harmful apps, etc. aiding preventive policing.

b. Real-time cyber patrolling to detect malicious IPs, phishing domains and harmful mobile/desktop applications.

c. Identifying new cyber threats & malicious software such as APKS, EXE, etc. and issue guidelines and SOPs for Government IT infrastructure.

ix. **Security & Network Operations Centre (SNOC)**

a. Round-the-clock monitoring of J&K Police's digital infrastructure.

b. Providing firewall and intrusion detection for O3C and S-DISC & EO Police Stations.

c. Monitoring all digital assets using SIEM platforms.

d. Conducting vulnerability scans and applying patch updates.

e. Alerting stakeholders about attempted breaches, compromised systems, or suspicious activity.

x. **Computer Emergency Response Team (CERT)**

a. CERT is a specialized unit which will be responsible for cyber security auditing of State's Cyber infrastructure.

b. The unit will formulate SOPs pertaining to Cybersecurity for stakeholders.

c. It shall coordinate with national CERT-IN and private security partners for intel sharing.

d. It shall conduct mock drills and simulation exercises.

e. It shall also prepare monthly threat bulletins.

xi. **AI-Driven Predictive Policing Unit**

The AI-Driven Predictive Policing Unit shall be established to address the emerging challenges arising from the use and misuse of Artificial Intelligence (AI) in cyberspace. The Unit shall perform the following functions:

a. Monitoring emerging trends related to AI in cybercrime and cyber-enabled offences.

b. Identifying, analyzing and tracking AI-enabled threats such as deepfakes, voice cloning, synthetic media, identity impersonation, AI-generated fraudulent content and other emerging forms of cybercrime.

c. Providing technical assistance to investigating officers in detection, examination and investigation of offences involving AI-generated content and AI-assisted criminal activities.

d. Recommending preventive measures, technological solutions, guidelines and best practices to counter the misuse of AI and strengthen cyber resilience across Jammu & Kashmir.

### C. Legal and Prosecution Support

This unit shall provide legal guidance to investigators throughout the investigation cycle. It shall assist in preparation of legal documents, scrutiny of case files, coordination with prosecutors and monitoring of trial proceedings. The unit shall ensure compliance with legal and procedural requirements.

## III. <u>Cyber Operations Wing</u>

The Cyber Operations Wing functions shall be headed by an SSP rank officer and serve as the central command and coordination unit for cybercrime response, cybersecurity operations, financial fraud mitigation, incident handling, research & innovation, public outreach & awareness, data aggregation & analysis, proactive threat generation and mitigation. The Wing shall ensure efficient coordination between

operational units, technical divisions, financial institutions, telecom service providers, and law enforcement agencies. This Wing will also be nodal for cyber slavery. This unit shall include:

**A. 1930 Call Center**

The 1930 Helpline shall be headed by a DySP rank officer. This Helpline, already functional on a 24x7 basis at CICE, Jammu serves as the primary citizen contact point for reporting cyber financial frauds. Upon receiving calls from complainants, the Helpline call receiver collects the necessary details of the incident and registers the complaint on the Cyber Police Portal for further processing and undertakes real-time coordination with banks, financial institutions, payment gateways & wallet service providers through the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) for prompt freezing of fraudulent transactions and mitigation of financial losses.

This division shall also ensure:

i. **Processing of e-Zero FIRs:** This unit shall ensure immediate registration and processing of cybercrime complaints irrespective of territorial jurisdiction through virtual police station. The primary objective shall be preservation of evidence and prompt initiation of legal action. The unit shall facilitate seamless transfer of cases while maintaining continuity of investigation.

ii. **Cyber Frauds Mitigation Centre (CFMC):** The CFMC shall function as the dedicated unit for minimizing financial losses arising from cyber frauds. It will have the representative of banks, payment gateways, financial institutions, TSPs in a building along with 1930 Helpline. The SOP for NCRP-CFCFRMS, Custody, Restoration of money and Grievance Redressal, issued by I4C dated 02.01.2026 shall be followed.

iii. **Cybercrime Helpdesk:** The Cybercrime Helpdesk shall act as a citizen facilitation and support unit for cybercrime victims. It shall assist complainants in filing NCRP complaints, guide them regarding evidence preservation, provide awareness on cyber safety measures, support vulnerable sections of society, and facilitate communication between complainants and investigating agencies. The helpdesk shall also monitor complaint status and provide support for grievance.

**B. Cyber Threats Division**

The Cyber Threats Division shall function as the intelligence and early warning unit of the JK4C. The Division shall be responsible for monitoring cyber threats, analyzing cybercrime trends, identifying emerging risks and generating actionable intelligence to support investigations, operations and informed decision-making. The Division shall maintain coordination with financial institutions, telecom service providers, internet intermediaries and law enforcement agencies for timely exchange of information and threat indicators. It shall be headed by an officer of the rank of Addl. SP/ DySP and shall comprise the following units:

i. **Research & Innovation Unit:** The Research & Innovation Unit shall function as the knowledge and innovation hub of the JK4C. It shall be responsible for conducting research on emerging cyber threats, evolving cybercrime trends, new technologies and changing criminal methodologies to support evidence-based decision-making and strategic planning. The Unit shall undertake studies

aimed at developing new investigative methodologies, best practices and SOPs for cybercrime investigation and digital evidence handling. It shall promote the use of AI, Machine Learning (ML), Data Analytics and other advanced technologies to enhance detection, threat analysis, intelligence generation and operational efficiency. Further, the Unit shall conduct policy research, prepare analytical reports and provide recommendations for strengthening cyber policing, cybersecurity and cyber resilience within the UT of Jammu & Kashmir.

ii. **Data Aggregation, Analysis & Proactive Threat Mitigation Unit:** The Data Aggregation, Analysis & Proactive Threat Mitigation Unit shall function as the central intelligence, analytical and early warning unit of the Cyber Threat Division under the JK4C. It shall be responsible for collecting, aggregating and analyzing information relating to cybercrime complaints, cyber frauds, cyber threats and other relevant intelligence received from law enforcement agencies, government departments, financial institutions, telecom & internet service providers, social media platforms and other authorized sources. Its primary objective shall be to identify cybercrime trends, fraud patterns, emerging threats, vulnerabilities and organized criminal networks operating within and outside the UT.

   a. The Unit shall maintain and continuously update centralized databases of cybercrime incidents, suspicious bank accounts, mobile numbers, malicious websites, phishing links, fraudulent digital assets, compromised infrastructure and other cyber threat indicators. Through data-driven analysis and intelligence correlation, the Unit shall prepare threat assessments, intelligence reports, analytical briefs and strategic inputs to support intelligence-led policing, operational planning, investigation and policy formulation.

   b. Based on the analysis of available intelligence and threat indicators, the Unit shall function as the UT's cyber early warning mechanism by preparing and disseminating timely alerts, advisories and notifications relating to emerging cyber threats, phishing campaigns, malware and ransomware attacks, online financial frauds, data breaches and vulnerabilities affecting government systems, critical infrastructure and citizens. Such alerts and advisories shall be disseminated to government departments, law enforcement agencies, financial institutions, telecom operators, internet service providers, other stakeholders and the public through appropriate communication channels. The Unit shall also maintain a repository of all alerts, advisories and threat notifications and periodically assess their effectiveness in enhancing cyber awareness, preparedness and resilience across Jammu & Kashmir.

iii. **Public Outreach/Awareness Unit:** The Public Outreach Unit shall be responsible for promoting cyber awareness and fostering safe digital practices among citizens across Jammu & Kashmir. The Unit shall design and implement cyber awareness campaigns to educate the public about emerging cyber threats, online frauds, phishing attacks, social media misuse, cyber bullying, identifying theft and other cyber-enabled crimes. The Unit shall conduct regular outreach programs in schools, colleges, universities, government institutions and private organizations to enhance cyber literacy and promote responsible use of digital technologies. It shall also undertake citizen awareness initiatives through

workshops, seminars, community engagement programs and awareness drives in urban as well as rural areas. Further, the Unit shall leverage social media platforms, digital media and other communication channels for dissemination of advisories, awareness content and preventive measures, thereby strengthening cyber hygiene and reducing victimization across the Union Territory.

### C. Cyber Security Division

The Cyber Security Division shall be headed by a DySP rank officer and shall be responsible for monitoring, preventing, and responding to cyber security threats affecting government systems, critical infrastructure, and public digital assets. The Division shall conduct vulnerability assessments, cyber audits, threat intelligence analysis, security monitoring, incident management, and awareness initiatives to strengthen cyber resilience and preparedness. Under this Division, the following units shall operate:

i. **Network Operations Centre (NOC) / Security Operations Centre (SOC):** The NOC/SOC shall provide continuous monitoring of networks, servers, applications, security devices, and digital infrastructure. The Center shall detect security incidents, analyze logs, generate alerts, monitor cyber security posture, and support incident response operations through centralized surveillance and real-time threat detection capabilities.

ii. **Cyber Commandos:** Cyber Commandos trained by the 14C, Ministry of Home Affairs, shall be deployed in the JK4C to strengthen cybercrime prevention, investigation, threat intelligence, incident response, and digital forensics capabilities. Their specialized training and technical expertise shall enhance the Centre's operational effectiveness in addressing emerging cyber threats and coordinating cybercrime response across the State/UT.

iii. **Preventive Security Unit:** The Preventive Security Unit shall focus on proactive cybercrime prevention through awareness campaigns, capacity-building programs, cyber hygiene promotion, advisory issuance, and stakeholder engagement. The unit shall identify emerging threats and vulnerabilities and develop preventive measures to reduce risks across government institutions and the public.

iv. **Incident Response Unit:** The Incident Response Unit shall provide rapid technical and operational response to cyber incidents, security breaches, malware infections, and digital emergencies. The unit shall conduct preliminary technical assessments, coordinate containment and recovery activities, support forensic acquisition, maintain incident response procedures, and liaise with national cyber response agencies when required.

## IV. OCWC Wing

With the rapid expansion of digital media across the country, women and children have become especially vulnerable to online crimes such as dissemination of non-consensual intimate images (NCII), cyberstalking, sextortion, grooming, cyber enabled human trafficking, circulation of child sexual cyber-enabled human trafficking, circulation of child sexual exploitation & abuse material (CSEAM) and technology facilitated gender-based violence.

Children are increasingly being victimized online in various ways due to their exposure to internet-based platform. Further, technology driven AI generative content

has because a double-edged sword. AI is being increasingly misused to generate explicit content, making it easier for perpetrators to produce and distribute CSEAM and sexually explicit content of women. Further, a growing challenge in the domain is live streaming sexual abuse of children (LSAC) and financial extortion of children (FSEC).

Under Project Surakshini of I4C, there is an active role of all stakeholders in combatting OCWC by Onboarding of IT intermediaries (preferably through APIs) Project SURAKSHINI will ensure the active role of all stakeholders in combatting OCWC. The proposed deliverables of this project include:

i. All complaints received on NCRP and pushed to the states and UTs through the cyber police portal will be analysed using the Proactive Monitoring Tool (PMT) for identifying the nature of digital content for taking appropriate action. The I4C and Law Enforcement Agencies will initiate action on the identified content and associated identifiers.

ii. Development of Prevention and Mitigation System (PMS) and setting up of a Prevention and Mitigation Centre (PMC) for OCWC. A landing page will be available on a newly developed PMS where all such flagged content and its action taken/to be taken, will be displayed in real time.

iii. This PMS will onboard all stakeholders like LEAs, Social media intermediaries, Internet service providers, etc., who will work in real time in ensuring timely action on flagged/reported content and associated coordination for timely enforcement.

iv. An OCWC dashboard will be created to analyse the data from the PMS in a more efficient manner.

To achieve the above deliverables, I4C, MHA envisages the establishment of OCWC Units in every State/UT police setup. These will function as specialized cells to handle NCRP complaints, intelligence gathering, operations against online sexual predators, investigations, prosecution support, and policy-level inputs for appropriate interventions.

**The following shall be the Objectives of the JK4C OCWC wing**

i. Ensuring timely action on NCRP complaints & tiplines.
ii. Providing intelligence reports of such organized online crime networks and hot spot clusters.
iii. Providing data-led inputs using NCRP complaints, Surakshini dashboard and CCTNS crime data for policy level intervention.
iv. Enhancing operational capacity for tracking, identifying, investigating and prosecuting online sexual offenders.
v. Strengthening inter-department coordination against online crime and exploitation networks.
vi. Creating a survivor-support ecosystem integrated with legal, counselling, and rehabilitation services.

## Annexure A1

| S. No. | Designation | Resources Required |
|---|---|---|
| 1 | Cyber Resource Centre - Core Unit | |
| | i. Centre Head/Senior Cybercrime Expert | 1 |
| | ii. Cybercrime Team Leader | 1 |
| | iii. Cybercrime Team Member | 1 |
| | iv. Cyber Law Expert | 1 |
| | v. Data Analyst | 1 |
| | vi. System/Database Administrator | 1 |
| | vii. IT Specialist (Jr. Level)- Hardware | 1 |
| | viii. IT Specialist (Jr. Level)- Software | 1 |
| 2 | Cyber Forensic Unit | |
| | i. Digital Forensics Expert | 1 |
| 3 | Mobile & Smartphone Forensic Unit | |
| | i. Smartphone Forensics Expert | 1 |
| 4 | Social Media & OSINT Unit | |
| | i. Sr. Social Media Analyst | 1 |
| | ii. Social Media Analyst | 2 |
| | iii. OSINT Analyst | 1 |
| 5 | Dark Web & Deep Web Analysis Unit | |
| | i. Dark Web & Deep Web Analyst | 1 |
| 6 | Blockchain & Cryptocurrency Analysis Unit | |
| | i. Block Chain Analyst | 1 |
| 7 | Data Aggregation & Analytics Unit | |
| | i. Data Analyst | 2 |
| 8 | Cyber Security Unit | |
| | i. Sr. Cyber Security Expert | 1 |
| | ii. Cyber Security Expert | 1 |
| 9 | Cyber Threat Analysis Unit | |
| | i. Cyber Threat Analyst | 1 |
| 10 | Computer Emergency Response Team | |
| | i. Cyber Security Analyst | 1 |
| 11 | Cyber Safety & Awareness Unit | |
| | i. Capacity Building Expert | 1 |
| 12 | Cyber Capacity Building Unit | |
| | i. Trainer | 3 |
| | ii. Coordinator | 1 |
| | iii. Curriculum Design Expert | 1 |
| 13 | Counsellors for OCWC | 6 |
| | Total | 34 |

## Annexure A2

| S. No. | Designation | Resources Required |
|---|---|---|
| 1 | Cyber Operations Wing, JK4C J&K | |
| | A. 1930 Call Centre: | |
| | ii. Cyber Fraud Mitigation Centre (CFMC) | |
| | a. Centre Head/ Team Leader | 1 |
| | b. Cyber Law Expert | 1 |
| | c. Data Analyst | 4 |
| | B. Cyber Threats Division: | |
| | ii. Data Aggregation Analysis & Proactive Threat Mitigation Unit: | |
| | a. Centre Head/ Team Leader | 1 |
| | b. Sr. Cyber Security Expert | 2 |
| | c. Data Analyst (Big Data Expert) | 3 |
| | d. Financial Data Specialist (Analyst) | 2 |
| | e. TSP/ISP/IMS/TMS Data Analyst | 2 |
| | f. Dark Web & Deep Web Analyst | 2 |
| | g. Sr. Social Media Analyst/OSINT Expert | 4 |
| | C. Cyber Security Division (24x7 ops): | |
| | i. Security and Network Operation Centre-Team Leader | 2 |
| | a. Network Security Engineer (NoC)-L3 Level | 3 |
| | b. Security/ Event Analysis Engineer (SoC)-L3 Level | 3 |
| | | |
| | Total | 30 |