



The Arunachal Pradesh Gazette

EXTRAORDINARY

PUBLISHED BY AUTHORITY

No. 218, Vol. XXXIII, Naharlagun, Wednesday, July 29, 2026, Sravana 7, 1948 (Saka)

GOVERNMENT OF ARUNACHAL PRADESH
DEPARTMENT OF HOME
CIVIL SECRETARIAT
ITANAGAR

NOTIFICATION

The 23rd July, 2026

No. HOME-12046/4/2026/739.—The Hon'ble Supreme Court of India, in *Suo Moto Writ Petition (Criminal) No. 03 of 2025*, vide Order dated 1st December, 2025, directed all State Governments and Union Territories to establish and operationalise Regional/State Cyber Crime Coordination Centres (R4Cs/S4Cs). Accordingly, the Ministry of Home Affairs, Government of India, established the Indian Cyber Crime Coordination Centre (I4C) as the national framework for a coordinated response to cyber crime and issued advisories to all States and Union Territories to strengthen State-level cyber crime coordination, monitor cyber crime complaints and facilitate inter-State and international cooperation.

In compliance with the aforesaid directions of the Hon'ble Supreme Court of India and in accordance with the policy framework of the Ministry of Home Affairs, Government of India, the Governor of Arunachal Pradesh is pleased to notify the establishment of a State-level cyber crime coordination mechanism to ensure decentralised investigation with centralised coordination, to be known as the **Arunachal Pradesh Cyber Crime Coordination Centre (AP4C)** at the State level and the **District Cyber Crime Coordination Centres (D4Cs)** at the district level.

Arunachal Pradesh Cyber Crime Coordination Centre (AP4C) shall function as the exclusive State-level cyber crime coordination centre, with its headquarters at Police Headquarters (PHQ), Itanagar. The **Deputy Inspector General of Police (Crime)** shall be the Head of AP4C, while the **Superintendent of Police, Cyber Crime**, stationed at Chimpu, shall serve as its Operational Head and shall be responsible for the overall supervision and coordination of all cyber crime-related matters.

AP4C shall not undertake investigations directly. Its mandate shall include the overall supervision and monitoring of cyber crime management in the State; coordination and correspondence with the Indian Cyber Crime Coordination Centre (I4C), the Ministry of Home Affairs (MHA), and other national agencies; monitoring trends emerging from the National Cyber Crime Reporting Portal (NCRP), the 1930 Cyber Helpline and the Cyber Crime Investigation Assistance Request (CIAR) system; facilitating inter-district and inter-State coordination; formulating and disseminating policies, Standard Operating Procedures (SOPs), advisories, and best practices; conducting capacity-building, training and public awareness programmes; and periodically reviewing the performance of the District Cyber Crime Coordination Centres (D4Cs) and the State Nodal Cyber Crime Police Station (CCPS), Itanagar.

1. Objectives :

The objectives of AP4C shall be as follows :

- To ensure effective coordination, analysis and response to cyber crime throughout the State.
- To monitor the investigation of cyber crime cases and complaints received through online platforms, including the National Cyber Crime Reporting Portal (NCRP) and the 1930 Cyber Helpline, as well as complaints registered offline at Police Stations.
- To provide technical, analytical, and operational support for cyber crime investigations.
- To strengthen cyber crime prevention through awareness, training and capacity-building initiatives.
- To facilitate the freezing, reversal and restoration of defrauded funds to victims, wherever legally permissible.

- (f) To function as the State Nodal Interface for coordination with national and international cyber crime coordination mechanisms.

2. **Functional Wings :**

AP4C shall comprise the following three functional wings :

- (I) **Cyber Administration and Governance Wing (CAGW)**
- (II) **Cyber Operations Wing (COW) / State Nodal Cyber Crime Police Station**
- (III) **District Cyber Crime Coordination Centre (D4C)**

I. **Cyber Administration and Governance Wing (CAGW) :**

The Cyber Administration and Governance Wing (CAGW) shall be headed by an officer of the rank of Inspector and shall function under the direct supervision of the Superintendent of Police, Cyber Crime and the Deputy Superintendent of Police, Cyber Crime, stationed at Chimpu.

The Wing shall perform the following functions:

- (i) To coordinate and facilitate training programmes by utilising the expertise available at CCPS, Itanagar, or from other competent agencies and institutions.
- (ii) To function as the State Nodal Unit for the Grievance Redressal Module (GRM) and the Money Restoration Module (MRM).
- (iii) To operate the 1930 Cyber Helpline and the National Cyber Crime Reporting Portal (NCRP) Coordination Unit through a dedicated team headed by an Inspector.
- (iv) To function as the Information, Education and Communication (IEC) Unit for cyber crime awareness and public outreach.
- (v) To function as the Cyber Security and Incident Response Cell by leveraging the technical expertise of CCPS, Itanagar. The Cyber Commando Unit shall provide operational support for cyber incident response and cybersecurity-related matters.
- (vi) To function as the Cyber Crime Support Cell.
- (vii) To function as the High Value Cyber Fraud Cell. Cases requiring investigation by the State Nodal Cyber Crime Police Station shall be referred to CCPS, Itanagar, in accordance with the prescribed jurisdiction.
- (viii) To function as the Inter-State and International Coordination Unit, including liaison with authorities under the Mutual Legal Assistance Treaty (MLAT) mechanism and Bharat Pol.
- (ix) The Cell shall maintain close coordination with the District Cyber Crime Coordination Centres (D4Cs) and District Social Media Monitoring Teams and shall facilitate the blocking or removal of malicious accounts, posts, or content through the Sahyog Portal, in accordance with applicable laws and prescribed procedures.
- (x) To function as the State Nodal Unit for the Sahyog Portal.
- (xi) To establish and operate the Cyber Crime Mitigation Centre (CCMC), which shall coordinate with banks, financial service providers, Telecom Service Providers (TSPs), Internet Service Providers (ISPs) through the Cyber Crime Mitigation Centre Unit (CMCU), and other stakeholders on behalf of the State for the prevention, detection and mitigation of cyber crime. The Centre shall be made operational in a phased manner, as and when required.
- (xii) To function as the State Cyber Crime Records Bureau.
- (xiii) To undertake all correspondence with the Ministry of Home Affairs (MHA), the Indian Cyber Crime Coordination Centre (I4C), the District Cyber Crime Coordination Centres (D4Cs), Police Headquarters (PHQ), and other concerned agencies. The Wing shall also be responsible for maintaining all records relating to the aforesaid functions.

II. **Cyber Operations Wing (COW)/State Nodal Cyber Crime Police Station :**

The Cyber Operations Wing (COW), comprising the State Nodal Cyber Crime Police Station, shall be headed by the Officer-in-Charge of the State Nodal Cyber Crime Police Station, Itanagar, who shall preferably be an officer of the rank of Deputy Superintendent of Police. The Wing shall function under the direct supervision of the Superintendent of Police, Cyber Crime.

The Cyber Crime Police Station (CCPS), Itanagar, shall function as the State-level specialised investigation unit. It shall investigate all financial cyber fraud cases involving amounts of **₹10 lakh and above**, irrespective of the district in which the offence occurred. CCPS shall also investigate complex, sensitive, organised, inter-district and inter-State cyber crime cases, as assigned or reviewed by AP4C and shall provide technical and investigative assistance to the District Cyber Crime Coordination Centres (D4Cs), as and when required.

The Wing shall perform the following functions :

- (i) To function as the Cyber Threat, Mitigation and Intelligence Cell.
- (ii) To maintain the Cyber Commando Unit, which shall serve as the State's emergency cyber response team. The Unit shall provide specialised training in emerging cyber crime techniques and technologies, including cryptocurrency investigations, blockchain analysis, APK application analysis, Artificial Intelligence (AI), digital forensics and cybersecurity operations and shall support the Cyber Security Wing as required.
- (iii) To provide technical, forensic and investigative assistance to the District Cyber Crime Coordination Centres (D4Cs) and AP4C whenever expert review or specialised support is required.
- (iv) To function as the State Nodal Unit for Online Crimes Against Women and Children (OCWC), including management of the Cyber Tipline and the CPRGR Portal and to supervise and monitor the functioning of the OCWC Units established in the districts.

III. District Cyber Crime Coordination Centre (D4C) :

A District Cyber Crime Coordination Centre (D4C) shall be established in the office of the Superintendent of Police in each district. The D4C shall function under the supervision of the Superintendent of Police. The Deputy Superintendent of Police, where designated, shall oversee its day-to-day functioning.

Functional Components of the District Cyber Crime Coordination Centre (D4C).

- (i) The District Cyber Crime Coordination Centre (D4C) shall function under the supervision of the Superintendent of Police and shall coordinate cyber crime prevention, detection, registration, investigation and prosecution of cyber crime cases, as well as activities relating to cybersecurity within the district.
- (ii) The D4C shall provide technical, analytical and operational support in matters relating to cyber crime. However, it shall not investigate cyber crime cases directly, except where specifically authorised under law or by the competent authority.
- (iii) The local Law and Order Police Stations shall be the Police Stations within the meaning of **Section 2 (1)(u) of the Bhartiya Nagarik Suraksha Sanhita, 2023 (BNSS, 2023)** for the purpose of registration and investigation of cyber crime cases falling within their respective jurisdictions.
- (iv) The D4C shall prepare and submit special and periodic reports to the **Deputy Inspector General of Police (Crime), Head of AP4C** and shall carry out such directions as may be issued by AP4C under the supervision of the respective Superintendent of Police.
- (v) The D4C shall monitor all cyber crime complaints received within the district through the **1930 Cyber Helpline**, the **National Cyber Crime Reporting Portal (NCRP)**, or any other recognised reporting mechanism and shall ensure that such complaints are pursued to their logical conclusion.
- (vi) The D4C shall coordinate with AP4C, banks, financial service providers, Telecom Service Providers (TSPs), Internet Service Providers (ISPs) through the Cyber Crime Mitigation Centre Unit (CMCU), and other stakeholders on behalf of the district for the prevention, detection, mitigation and investigation of cyber crime.
- (vii) The D4C shall generate cyber crime-related intelligence through the use of technical resources, cyber analytics, digital tools and field operations and shall disseminate actionable intelligence to the concerned investigating agencies whenever required.
- (viii) The D4C shall organise and facilitate the training of police personnel involved in the investigation and prosecution of cyber crime cases within the district. The **CyTrain Portal** and other approved training platforms shall be utilised for this purpose.
- (ix) The D4C shall organise and participate in programmes for creating public awareness regarding cyber threats, cyber crime prevention and cyber hygiene in collaboration with Government departments, educational institutions, financial institutions and other Government and non-governmental organisations.
- (x) The **Police Station at district Headquarters** shall establish a **Cyber Cell** and every Police Station shall establish a **Cyber Help Desk**. The concerned **Officer-in-Charge** shall function as the Operational Head of the Cyber Cell/Cyber Help Desk. Subject to operational requirements and availability of resources, the Cyber Cells may be upgraded into full-fledged Cyber Crime Police Stations in the future.
- (xi) All financial cyber fraud cases involving amounts below **₹10 lakh** shall be registered and investigated by the jurisdictional Police Station with the technical and operational support of the D4C. The D4C shall facilitate the investigation of routine cyber crime cases of a local nature, ensure the effective utilisation of the National Cyber Crime Reporting Portal (NCRP) and allied portals, facilitate the timely freezing and restoration of defrauded funds, provide victim assistance and coordinate with AP4C and the Cyber Crime Police Station (CCPS), Itanagar, wherever necessary. The D4C shall also conduct cyber crime awareness and outreach programmes within the district, including the sensitisation of Police Stations, Government departments, educational institutions and the general public.

- (xii) **An Online Crimes Against Women and Children (OCWC) District Unit** shall be established in every district where a **Women Police Station (WPS)** is functional. The Unit shall manage the **Cyber Tipline** and the **CPRGR Portal**, investigate cases relating to Online Crimes Against Women and Children and perform such functions as may be assigned by AP4C. In districts where a Women Police Station is not available, these responsibilities shall be assigned to a designated woman police officer nominated by the Superintendent of Police.
- (xiii) The District Cyber Crime Coordination Centre (D4C) shall function as the district-level operational, coordination, facilitation and technical support unit for cyber crime prevention, detection, investigation support and victim assistance.

The functions of these components are specified in Annexure I and II, annexed hereto.

3. **Manpower and Flexibility :** The Head of AP4C shall be empowered to assign, reassign or rotate Police Inspectors and Police Sub-Inspectors within Cyber Crime Police Station to any wing or functional unit of AP4C with the consent of PHQ, based on operational requirements and expertise. A special recruitment drive shall be done in future with the technical background required for Cyber Crime Units till then AP4C and D4C shall draw manpower from the general pool of APP. The establishment of new wings and units shall be done as per the arising needs with the approval of the Government.
4. **Review and Reporting : -**
- (a) AP4C shall submit monthly operational and analytical reports during the review meeting of the Director General of Police, Arunachal Pradesh.
- (b) The functioning of AP4C may be reviewed quarterly by the Home Secretary.

The Arunachal Pradesh Cyber Crime Coordination Centre (AP4C) shall have jurisdiction over the entire State of Arunachal Pradesh and shall function as the nodal coordination, monitoring and response centre for cyber crime.

This Notification shall come into force with effect from the date of its publication in the Official Gazette.

By order and in the name of the Governor of Arunachal Pradesh.

Kaling Tayeng, IAS
Principal Secretary (Home),
Government of Arunachal Pradesh,
Itanagar.

Annexure-I

STAFFING PATTERN

Sl. No.	Components	Head	Operational Head	IO	EO	Establishment work	Data Operator	OCWC
1.	AP4C	DIG, Cyber Crime-1	SP, Cyber Crime-1 assisted by Dy SP-1					
2.	Cyber Administration and Governance Wing (CAGW)	Inspector-1	SI-3,			HC-4	Ct-15	
3.	1930, 24x7	SI -1	HC-1				Ct-8	Lct-4
4.	Cyber Operations Wing (COW)/State Nodal Cyber Crime Police Station	Dy SP-1 as an Officer in Charge		10 Inspectors as an IO and 4 lady Inspector for OCWC	6 SI assistance to IOs and 4 lady SI for OCWC	HC-4	Ct-30	Lct-5
5.	District Cyber-Crime Coordination Centre (D4C)	D4C at the SP office may be staffed as per the strength available to run the NCRP police portals. The District Nodal Office, GRM/MRM and Cyber Cell at the Police Station at the district headquarters may be staffed according to the strength available, with a minimum of 1 Inspector, 1 SI, and 4 constables to look after the portals, registration of cases in NCRP, GRM/MRM (money restoration) and the OCWC Unit. The OCWC Unit at the WPS, or, if there is no WPS in the district, the Police Station at the district headquarters shall look after the OCWC Unit, staffed with lady officers.						
6.	Total	DIG-1	SP-1	Dy. SP-2	Inspectors -20	HC-13	Ct-63	

Annexure - II

