

Government of Gujarat

No. HD/CYC/e-file/8/2026/1764/SB4

Home Department,
Sachivalaya, Gandhinagar.

Date: **25 MAY 2026**

Read

1. Ministry of Home Affairs, CIS Division, CIS.III desk, Government of India's letter No. 22003/05/2019-CIS-II dated 23/09/2019.
2. Home Department, Government of Gujarat's resolution no. MHK/102012/3580/C dated 03/05/2013.
3. Home Department, Government of Gujarat's resolution no. HD/MHK/e-file/8/2025/0256/C dated 09/04/2025.
4. Proposal of Director General of Police, CID Crime and Railways, Gujarat State vide letter No. DGPCR/0533/01/2026 dated 17/01/2026.

Preamble

The rapid expansion of digital technologies, internet penetration, online financial systems, cloud computing, artificial intelligence and social media platforms has transformed governance, commerce, communication and service delivery. While this digital transformation has created significant opportunities for economic growth and social inclusion, it has also led to emerging cyber threats.

In recent years, India has witnessed a notable rise in cyber crimes such as online financial frauds, phishing attacks, ransomware, identity theft, non-consensual dissemination of intimate imagery, digital arrest scams and social media exploitation, largely driven by increased digital payments, smartphone usage and expanding online services.

To address the increasing challenges of cyber crimes, in line with the instructions of the Ministry of Home Affairs, Government of India, to establish Cyber Crime Coordination Centres in coordination with the Indian Cyber Crime Coordination Centre (I4C) vide letter referred at Read (1) the Government of Gujarat, has exercised the 'State Cyber Crime Cell' at Karmayogi Bhavan, Gandhinagar vide Resolution referred at Read(2), which is functioning as a separate unit under the Office of CID Crime & Railways, Gandhinagar, to address cyber crimes and also acts as the nodal agency of the Indian Cyber Crime Coordination Centre (I4C) in the State of Gujarat, and The Superintendent of Police, State Cyber Crime Cell, is designated as the State Nodal Officer for coordination with I4C.

Cyber offences today are increasingly technology-driven, trans-national and complex, often involving tools such as malware, encrypted platforms, dark web networks and AI-enabled fraud mechanisms. Investigation and prevention of such offences require specialized technical expertise, advanced digital forensic capabilities and continuous capacity building of law enforcement agencies.

The Government of Gujarat has strengthened the cyber policing framework in the State through the establishment of the State Cyber Crime Cell and Cyber Crime Police Stations across the districts. However, in view of the evolving cyber threat landscape and the increasing volume and complexity of cyber crimes, it has become necessary to develop a more advanced cyber policing mechanism to support research, training, technological development and advanced investigation capabilities in the State.

In order to address the emerging cyber crime challenges and strengthen the cyber policing ecosystem in the State, and in pursuance of the budgetary provision for FY 2025-26, the Government of Gujarat has approved the project titled 'Cyber Centre of Excellence (CCoE)' to support law enforcement through advanced research, training, technological development, digital forensic support and capacity building, including the required manpower and infrastructure, vide resolution referred at read (3), and accordingly the establishment

of the 'Cyber Centre of Excellence (CCoE)' was under active consideration of the Government of Gujarat.

Resolution

After careful consideration, the Government of Gujarat hereby resolves to establish the 'Cyber Centre of Excellence (Cyber CoE), Gujarat', as a specialized cyber policing institution to strengthen the State's capabilities in the areas of cyber crime prevention, detection, investigation and research, cyber intelligence, cyber forensics, cyber awareness, and policy support. The details of the Cyber Centre of Excellence (Cyber CoE) are as under:

1. Title and Status

- I. The institution shall be known as "**Cyber Centre of Excellence, Gujarat**" (hereinafter referred to as "**Cyber CoE, Gujarat**").
- II. It shall be located at a place as may be decided by the Government of Gujarat.
- III. It shall function as a State-level apex institution to support law enforcement agencies in addressing emerging cyber threats in Gujarat.
- IV. It shall function under-
 - i. **Overall supervision of the Director General of Police & HoPF, Gujarat State.**
 - ii. The **immediate administrative control** shall vest with the **Additional Director General of Police (Cyber CoE)**; in the absence of an officer of the said rank, the same shall be exercised by the **Inspector General of Police or Deputy Inspector General of Police (Cyber CoE)**.
- V. It shall supervise, provide support and have generalized control over-
 - i. All Range and Commissionerate cyber cells and cyber police stations,
 - ii. All District cyber cell, cyber labs and cyber police stations,
 - iii. Any other jurisdictional or specialized cyber crime division - **functioning in Gujarat State.**
- VI. Existing Cyber arm '**State Cyber Crime Cell, CID Crime & Railways, Gujarat**' placed at Karmayogi Bhavan, Gandhinagar **shall be merged in Cyber CoE, Gujarat.**
- VII. It shall act as Gujarat cyber crime coordination centre (G4C) and will serve as **state nodal agency of Indian cyber crime coordination centre (I4C).**
- VIII. The immediate administrative controlling authority of the Cyber CoE shall be **designated as the State Nodal Officer for coordination with I4C.**

2. Objectives and Functions

The Cyber CoE, Gujarat shall undertake the following objectives and functions:

- I. To strengthen the State's institutional capacity for prevention, detection and investigation of cyber crimes.
- II. To provide technical, analytical and digital forensic support to law enforcement agencies in cyber crime investigation and digital evidence examination.
- III. To develop capabilities in cyber intelligence, cyber threat analysis and cyber security support for effective cyber policing.
- IV. To undertake research and development on emerging cyber threats, technologies and investigation methodologies, and to promote technological innovation in cyber policing.
- V. To conduct specialized training, capacity building programmes and knowledge-sharing initiatives for police personnel and other stakeholders.
- VI. To develop tools, methodologies, standard practices and technological solutions for cyber crime investigation and digital evidence management.
- VII. To promote cyber safety awareness and preventive initiatives for citizens and organizations.

VIII. To provide policy support and strategic inputs to the Government in matters relating to cyber crime and cyber security.

3. Mandate and Supervisory Authority

The Cyber CoE-

- I. Shall serve as Gujarat State's apex body for cyber crime prevention, detection, investigation, research, training, cyber intelligence, cyber forensics, cyber awareness, and policy support.
- II. Shall supervise, monitor, and provide technical guidance for cyber crime investigations, crime prevention, security, and awareness activities undertaken by the entities referred to in para 1.V.
- III. Shall ensure standardized procedures, technical uniformity, and operational coordination across the entities referred to in Para 1.V.
- IV. Shall provide continuous technical oversight, capacity building, and quality assurance for cyber crime operations, cyber forensic examinations, cyber intelligence collection, and cyber awareness initiatives undertaken by the entities referred to in para 1.V.
- V. Shall establish a Cyber Security Centre to provide cyber security services to Government and private sector entities on a revenue-based framework, as may be determined in consultation with the Government of Gujarat.
- VI. Shall obtain periodic reports (daily/weekly/monthly) from all entities referred to in Para 1.V and prepare a consolidated monthly & annual report for submission to the Government of Gujarat.
- VII. The immediate administrative controlling authority of Cyber CoE shall conduct the performance appraisals of officers (PI, DySP, ACP, DCP) posted in entities referred to in Para 1.V.
- VIII. The immediate administrative controlling authority of Cyber CoE shall, in consultation with the DGP & HoPF, Gujarat State and the Home Department Gujarat, prescribe the methodology and conduct periodic inspections of the entities referred to in para 1.V, in accordance with the Gujarat Police Manual.

4. Organizational Structure

For effective discharge of its mandate, the Cyber CoE shall function through specialized operational, intelligence, security and training units working in an integrated manner to support cyber policing in the State. The organizational structure shall be as under:

Unit Name	Functions and Objectives of Unit
1. <u>CYFORCE</u> Cyber Crime Investigation Unit	It includes financial, non-financial, and high-end technical offenses like cryptocurrencies crimes, dark-web, etc. The unit will be divided into five zones, covering the entire state. • Centralized reference for all cyber-crimes in the state. • Streamlined command and control system. • Specialized teams for tackling cybercrime syndicates and neutralizing organized cyber threats. • Advanced operational intelligence and real-time situational awareness. • Cutting-edge digital forensic capabilities for cybercrime investigations. • Augmented Reality (AR) integration for field operations. • AI-driven behavioural pattern recognition and suspect profiling. • Cryptocurrency investigations, hacking incidents.

2. <u>CYINT</u> Cyber Intelligence & Threat Analysis Unit	Focused on Open-Source Intelligence (OSINT), Social Media Intelligence (SOCMINT), dark web surveillance, online illegal activities, and emerging cyber threats. Additionally, this unit oversees lawful technical interceptions of calls, data, and classified communications as permitted under applicable laws with a high degree of confidentiality. Financial intelligence gathering and inter-agency coordination will also be part of its mandate.
3. <u>CRIMENET</u> Human Trafficking, Narcotics, Organized Crimes & Anti-National Activities Monitoring Unit	Dedicated to tracking and investigating cyber-enabled human trafficking, narcotics networks, anti-national activities, financial cybercrimes, and organized criminal activities that leverage online transactions. This unit will ensure comprehensive coverage across the state. • Investigation of cyber-enabled narcotics trade and organized cybercriminal networks. • Financial transaction monitoring for cyber-enabled illicit trade and narcotics funding. • Comprehensive database tracking for cyber-enabled human trafficking investigations. • Identification and dismantling of cyber-enabled human trafficking networks. • Tracing financial trails related to cyber-enabled trafficking and organized crime. • Coordinating cyber-enabled counter-terrorism operations and radicalization monitoring. • Real-time surveillance of suspicious individuals and terrorist and other anti-national networks. • Strengthening cross-border cyber intelligence sharing and cooperation.
4. <u>AIPOL</u> AI-driven Predictive Policing Unit	Leveraging artificial intelligence to forecast crimes and profile potential suspects, thereby strengthening proactive policing measures. • Creation and utilization of a centralized cybercrime data bank for data mining, data fusion and analysis. • Implementation of predictive analytics for proactive law enforcement. • AI-powered crime forecasting and suspect profiling. • Strengthening future-proofing initiatives in cybercrime prevention. • Advanced analytics and big data processing for investigative insights. • Technical support in cybercrime investigations and real-time monitoring.

5. <u>CYSEC</u> Cyber Incident Response & Digital Security Unit	To secure against cyber warfare threats, responding to cyber incidents, and providing advanced threat mitigation strategies. • Collaboration with cybersecurity professionals and industry experts for robust cyber resilience. • Providing real-time, actionable intelligence for dynamic cyber threat response. • Advanced behavioural pattern analysis and suspect profiling for intelligence insights. • Supply chain forensics targeting global cyber threats, including botnet tracking. • Real-time detection and monitoring of cyberattacks. • Integration of cloud computing and edge intelligence for immediate cyber response. • Providing cyber security to government infrastructure and to private sector entities on a revenue-based framework subject to Government approval and in accordance with applicable financial regulations. • Central Forensic Lab.
6. <u>CYCORE</u> Cyber Training, Awareness & Administration	Specialized in training law enforcement personnel, enhancing investigative capabilities, and public awareness initiatives in cyber domains. • Specialized training programs to strengthen cyber investigation proficiency. • Development of targeted skill enhancement programs for cybercrime professionals. • Reader Unit. • All the existing units of Cyber Cell including Unfreeze and Refund Unit. • Creation of public awareness and training modules for law enforcement and citizens. • Development of cyber education materials and security awareness programs. • Managing all administrative functions, inter-agency collaboration, and resource allocation for cyber forensic investigations. • Coordinating with law enforcement agencies, industry experts, and national security bodies. • Ensuring optimal resource availability for digital forensic investigations. • Administrative management of cyber units, logistics, and legal compliance. • Servers and Smart Storage.

5. Training

In view of the escalating complexity of the digital threat landscape, the Centre of Excellence (CCoE) shall establish a structured training mechanism for police personnel deployed in cyber institutions across the State. The training programme shall include capacity building, periodic refresher courses, specialized technical modules and a standardized evaluation system to assess and certify the proficiency of personnel.

This mechanism shall be designed to facilitate continuous skill augmentation through specialized training modules, ensuring that the force remains adept at countering emerging cybercriminal methodologies. Furthermore, the Cyber CoE will implement a standardized evaluation system to formally assess and acknowledge the proficiency levels of all personnel, thereby ensuring a high-caliber, certified workforce capable of maintaining operational excellence in cyber forensics, cyber-investigations and other cyber domains.

6. Periodic Review

To maintain high performance, the work and strategic plans of the Cyber CoE will be reviewed through the following schedule:

- I. **Quarterly Reviews:** Progress and functional outcomes will be reviewed every three months by the Additional Chief Secretary / Principal Secretary (Home Department, Gujarat).
- II. **Half-yearly Reviews:** A high-level strategic review will be conducted every six months under the chairmanship of the Chief Secretary, Gujarat, to ensure the Cyber CoE is aligned with broader government policies and effectively coordinates with state's security goals.

7. Empowerment

The immediate administrative controlling authority of the Cyber CoE shall ensure that all entities under its control, specifically those referred to in Para 1.V and the Cyber CoE itself, have the requisite legal status, to function as police stations under applicable criminal laws, or other relevant statutes. The authority shall also ensure that this status may formally get notified by the competent Government, completing all necessary procedural requirements.

8. Financial Provision

Expenditure for the establishment and functioning of the Cyber CoE shall be met from budget provisions under the Home Department, Government of Gujarat, or through any other funding mechanisms approved by the Government.

The Home Department, Government of Gujarat, shall also conduct periodic reviews of such expenditure to ensure its proper utilization, efficiency, and alignment with the objectives of the Cyber CoE.

This resolution shall come into force from the date of its issuance.

By orders and in the name of Governor of Gujarat.


(Sanjeev Kumar)
Principal Secretary
Home Department
Government of Gujarat

To,

1. Principal Secretary to Hon'ble Governor, Raj Bhavan, Gandhinagar.
2. Principal Secretary to Hon'ble Chief Minister, Swarnim Sankul-1, Sachivalaya, Gandhinagar.
3. Additional Principal Secretary to Hon'ble Chief Minister, Swarnim Sankul-1, Sachivalaya, Gandhinagar.
4. Secretary to Hon'ble Chief Minister, Swarnim Sankul-1, Sachivalaya, Gandhinagar.

5. Personal Secretary to Hon'ble Deputy Chief Minister, Swarnim Sankul-1, Sachivalaya, Gandhinagar.
6. Personal Secretary to Hon'ble Minister of State (Home), Swarnim Sankul-2, Sachivalaya, Gandhinagar.
7. Personal Secretary to All Hon'ble Ministers, Government of Gujarat, Sachivalaya, Gandhinagar.
8. Personal Secretary to the Leader of Opposition Party in Gujarat Legislative Assembly, Gandhinagar.
9. Home Secretary, Ministry of Home Affairs, Government of India, North Block, New Delhi.
10. CEO, I4C, 5th Floor, NDCC-II Building, Jai Singh Road, New Delhi.
11. Additional Secretary to Chief Secretary, Government of Gujarat, Sachivalaya, Gandhinagar.
12. Secretary & RLA, Legal Department, Sachivalaya, Gandhinagar.
13. All Administrative Departments, Sachivalaya, Gandhinagar.
14. Director General of police and HoPF, Gujarat State, Police Bhavan, Gandhinagar.
15. Director General of police, CID Crime and railways, Gujarat State, Police Bhavan, Gandhinagar.
16. Inspector general of police, Cyber Centre of Excellence, Karmayogi Bhavan, Gandhinagar.
17. Superintendent of police, State cyber crime cell, Karmayogi Bhavan, Gandhinagar.
18. ** All Police Commissionerates, Gujarat.
19. ** All Police ranges, Gujarat.
20. ** All SP offices, Gujarat.
21. ** All District cyber police stations, Gujarat.
22. Director, Office of the Director of Prosecution, Karmayogi Bhavan, Sector-10, Gandhinagar.
23. Account General (A&E) Gujarat, Rajkot.
24. Account General (A&E) Gujarat, Ahmedabad.
25. Director, Account & Treasuries, Gujarat State, Gandhinagar.
26. Pay & Account Offices, Ahmedabad/ Gandhinagar.
27. Resident Audit Officer, Ahmedabad/Gandhinagar.
28. Deputy Secretary (TC&T), Home Department, Sachivalaya, Gandhinagar.
29. Under Secretary (Personnel), Home Department, Sachivalaya, Gandhinagar.
30. Section Officer, IT Branch, Home Department, Sachivalaya, Gandhinagar...with request to publish on Department's website.
31. Select File.

** Office of DGP & HoPF, GS is requested to circulate with concerned offices.



(Tanmay Patel)
Section Officer
Home Department
Government of Gujarat

