Police manual

CYBER CRIME

I. Introduction:

As per the directives of Supreme Court, Ministry of Women & Child Welfare, Women Safety Division of MHA jointly with Women Safety Division of MHA and CERT-In, Cyber Crime Cell / Cyber Lab were established focussing on the "Cyber Crime Prevention against Women and Children" (CCPWC), This includes with Toll Free Dial 1930 integrated with ERSS.

A. **Cyber Crime Cell** @ Cyber PS was created vide **GO. Ms. No. 56 / 2015 dt 19.08.15** and entrusted with CBCID PS and started functioning at CB CID PS.
B. **Cyber Lab** was established at 3rd Floor, multi-storied building, Gorimedu, Puducherry along with ERSS in September 2018 with the CSR fund by IOC, Villianour.
C. **Cyber PS integrated with Cyber Lab** was established and **started functioning independently** from 17.11.2022 in the **Ground Floor** of the same building, as per the directives of I4C, MHA.
D. **Registers / Records:** As like all Police Stations, Cyber PS will maintain all Police Station Records / Registers. In addition, it will maintain **Special Registers** for every Gadgets utilized in Cyber Lab, individual registers for every request for CDR, IPDR, Blocking, Freezing / Unfreezing etc as part of transparency.
E. **Cyber Forensic, FSL, Puducherry:** FSL Puducherry has started Cyber Forensic to support Cyber PS & other Police Stations in Puducherry UT
F. **Cyber Hub:** As per the directives of I4C and as like Kerala Police, as **PPP Model** – "Cyber Hub" was developed by coordinating with professional Colleges & Universities. MoU was signed with RRU and PTU while to be executed with PU and WEC.
G. **Cyber Volunteers:** About 300 students from different professional colleges were motivated to register themselves with I4C in addition with professionals & Volunteers
H. I4C & JCCT-6: As Cyber Crimes are committed by criminals with no border, Central Government **(Meity)** is extending all supports by forming a centralized database through **CERT-In** (Indian Computer Emergency Response Team). The CERT-In has formed
    1. **I4C** (**Indian Cyber Crime Coordination Committee**).
    2. I4C has formed 7 JCCT's (**Joint Cyber-Crime Coordination Teams**)
    3. Pondicherry is part of **JCCT - 6.**

2. Major Responsibilities

A. Registration & Investigation of Cyber Crimes:

All complaints against Cyber Crime will be attended covering all the **4 Regions.** Complaints will be registered in NCRP (National Cyber Crime Reporting Portal) for preliminary examination and then FIR in the CCTNS Police Portal. All Police Stations receiving Cyber Complaints will assist the complainant to register the Cyber Complaint in the citizen portal of Cyber Crime **"cybercrime.gov.in"** which will directly reach Cyber PS online and further action will be taken with automatically. Complaints will be supported by Screen Shots signed be the complainant u/s 65B IT Act. Sensitivity and openness to be adopted as per periodical guidelines of the Judicial Courts on the Freezing and Unfreezing of Bank accounts against Financial Fraud cases to avoid misuse & abuse which will be view seriously. **Lok Adalath Court** can be utilized for speedy disposal of Cyber cases as deems fit

B. **Complaint gateway** for citizen to lodge a complaint to cyber police likewise cyber police station to report the Cyber Crime with I4C as below.

Citizen	Complaint gate ways	**1) I4C –** a) Toll free 1930 b) cybercrime.gov.in c) Tipline - report.cybertip.org d) 112 -	• All complaints were scrutinized to filter false & cock-tail complaints. • If point of jurisdiction differs, then we assist citizen

		https://py.erss.in/wdt 2) Direct 3) Postal / Petition 4) Senior Officers 5) Email 6) LG PMS / CP Gram etc 7) CCTNS **8)** CEIR – Mobile Missing	to register his complaint in citizen portal
Police	Registering modes	1. NCRP cyberpolice.nic.in 2. FIR cctnspolice.py.gov.in	cyberpolice.nic.in portal developed by I4C is interoperable with other pillars (Service Providers) like Banks, ISPs, TSPs, Social Media Service Providers
I4C	Investigation	• **CIAR Website – Cyber Crime Investigation Assistance** Reporting coordinating with other States / UTs • Cyber Police, cyber accused Hot spot, etc	

C. Cyber Helpline No. 1930 integrated with Dial 112 @ ERSS @ CCR functioning in the 3rd Floor of the same complex. Dedicated extension will be extended by C-DAC, SDA for ERSS as per the directives of I4C with the fund allocated (34 Lakhs). All complaints received through 1930 & 112 are send to Cyber Crime PS and through web dispatcher (**https://py.erss.in/wdt)** and through Whatsapp. These are registered on the online portal **https://cyberpolice.nic.in** and forwarded to respective PS based on classification of offences.

D. **Cyber Attacks:** I4C / MieTY / CERT-In guidelines / SOPs to be followed and awareness to be created with all staffs by SHO. Special focus is **High End cyber-attacks** like "Hacking of Database" / Server" etc to be reported before CERT-In **immediately & directly** by the Victim marking copy to Cyber PS as per SOP.

E. Cyber Commando Force: I4C assisting every State / UT in the screening, training of willing volunteer Police personnel for the creation of Cyber Commando within the Police Force

F. Cyber Volunteers: SHO must encourage Students, Young professionals, etc to get registered themselves as Cyber Volunteers through **cybercrime.gov.in** website maintained by I4C. Volunteers for creating citizen awareness on Cyber Crime & assisting Cyber PS in solving crimes etc. These volunteers will act as Force Adds-on during contingencies. If any.

G. Make use of the **MoUs signed** with professional Universities like RRU, PTU, PU, Women's Engineering College, etc

H. Centralized Monitoring System (CMS)
Lawful Interception & Monitoring – Nodal is DoT. Puducherry acts as Client to Tamilnadu Circle by C-DOT. **Centralized Monitoring System (CMS)** for **Lawful Interception & Monitoring** by DoT. Instrumentations was procured. **Administrative Sanction** was obtained for Infrastructure and pending for **Expenditure Sanction**. After carrying out Infra structure works, installation will be don't by C-DOT. Latest compliance given Under Secretary (Home)

I. Social Media Monitoring Cell
Social Media Monitoring Cell to monitor ie., Facebook, Whatsapp, Twitter, Instagram and You-tube and to interact with the intermediaries to block the unlawful contents

J. Coordination with I4C, JCCT, MHA and maintenance of accounts & expenditure on Central Assistance

3. Investigation Assistance by I4C:

A. **I4C websites like "cyberpolice.nic.in" & CIAR extending all assistance to Investigation / Enquiry Officers** as like Interoperable like ICJS connecting with all Service Providers like Banks, ISP / TSPs, all Cyber Police Stations in India for speedy enquiry on cyber frauds etc, providing HOT Spot location of Cyber Criminals in mapping their locations based on the complaints registered with NCRP Website, seeking securing of local jurisdictional Cyber Criminals mapped in the "Hot Spot" and intimate the jurisdictional police through court, etc

B. Banks freezes accused account as 1st layer, and subsequent accounts of transactions as 2nd and 3rd layers etc only after registration of FIR. Utmost care will be ensured by IO / EO before freezing or blocking of SIM / IMEI / Websites etc. Follow up to ensure whether action was taken or not with the assistance provide by I4C.

C. IO will proceed following the NCRP Portal and seek additional information from the various service providers **(Intermediaries - ISP / TSP / Banks / Social Medias / etc)** in tracking the accused and removal of disputed / abusive contents and guide the victims to get redressal from Intermediaries through their **Customer Grievance Redressal portal**.

D. **SOP**'s, Guidelines, Orders issued for handling **Financial Frauds Cases** to be followed without any excuse.

E. **Fake / Hacking / objectional contents in Social Media Accounts:**

- **"Grievance Redressal"** mechanism of the respective Service Providers to be utilized by guiding the victim / complainant for blocking and recovering of the account.
- Block of **objectional contents** through **Nodal Officer @** SP (Cyber).
- IP details of accused where he hacked the account or posted the obscene @ objectional content

4. Major Investigation components in Cyber Crime

SN	3 Major Components
1	Machine to Machine links
2	Machine to real accused on both sides
3	Location of the accused
SN	**Preparing evidences**
1	Digital evidences within the scope of IT Act
2	List of Documents
3	Memo of evidences

5. I4C: **Hot Spot:** In Cyber Crime the word "Hot Spot" to be viewed differently as learnt from seniors in Cyber Crime is

A. Location of Cyber Criminals
B. From where / geo location / IP location / SIM location / SIM where purchased / URL @ website domain and Website IP
C. Likewise, Location of *ATM / Bank Accounts / POS etc* to be identified as *PRIMARY* part of Cyber Investigations.
D. Unlike *Incidents / Events* grouped with geo location by NCRB.
E. Cognisance of this will be taken up by JCCT"s / I4C functioning under CRRT-In.
F. Presently, Cyber Cell @ PS is equipped with **13 gadgets** needed for analysing Hard Disk / Mobile Phone & memory / IP Grabber / Mobile Tracking / etc. **List enclosed**.

6. Cyber related **cases** will be forwarded to Cyber PS, Puducherry for further investigation as per IT Act. Those cases will be investigations and disposed before the jurisdictional court.

7. As like normal Police Stations, Cyber PS will send all periodical and monthly reports and attend all periodical crime review meetings called by respective senior officers with special attention to DIG, IGP, DGP, etc.