



***RSLSA***  
***(Legal Services for  
Victims of Cyber Crimes)***

***Scheme, 2026***



# INDEX

| <b>S.No.</b> | <b>TOPIC</b>                                               | <b>PAGE</b> |
|--------------|------------------------------------------------------------|-------------|
| A            | INTRODUCTION                                               | <b>1</b>    |
| B            | WHAT IS CYBER CRIME                                        | <b>2</b>    |
| C            | CLASSIFICATION OF CYBERCRIME                               | <b>3-5</b>  |
| D            | IMPORTANT PROVISIONS IN VARIOUS LAWS RELATED TO CYBERCRIME | <b>6-7</b>  |
| E            | NAME OF THE SCHEME                                         | <b>7</b>    |
| F            | DEFINITIONS                                                | <b>7</b>    |
| G            | OBJECTIVES OF THE SCHEME                                   | <b>8</b>    |
| H            | CYBER REDRESSAL UNITS                                      | <b>9-18</b> |



## A. Introduction

The rapid expansion of digital technology has transformed modern life by enabling instant communication, online financial transactions, remote education, e-governance services, and widespread access to information. Today, a person can access banking facilities, government schemes, employment opportunities, and social interaction through a mobile device from virtually any location. While the internet has greatly improved efficiency, convenience, and economic participation, it has simultaneously created new vulnerabilities that are increasingly being exploited by cyber offenders.

The growing dependence on the internet, particularly for digital payments and online services, has led to a corresponding rise in cyber-related offences. A large section of the population has adopted online platforms without adequate awareness of basic digital safety practices. As a result, ordinary citizens are often exposed to financial fraud, identity theft, impersonation, online cheating, and data misuse. Cybercrime, therefore, is no longer confined to sophisticated computer systems; it now affects common users in their daily activities such as online banking, shopping, job searches, social networking, gaming, and data storage.

The use of the internet has undoubtedly improved the speed and efficiency of transactions and reduced procedural delays in many sectors. However, the same technological ease has also enabled offenders to commit crimes remotely, anonymously, and across territorial boundaries. Criminals exploit trust, fear, and lack of awareness rather than technical weaknesses alone. Consequently, cybercrime has emerged as one of the fastest-growing categories of crime in India.

According to data compiled by the Indian Cyber Crime Coordination Centre (I4C) and the National Cyber Crime Reporting Portal (1930 helpline), reported cyber-fraud losses exceeded ₹22,800 crore in 2024 and continued to rise sharply during 2025, with reported losses crossing ₹30,000 crore. Millions of complaints are now reported annually across the country. The increase is closely linked to the rapid expansion of digital payment systems, particularly Unified Payments Interface (UPI) transactions, which, while convenient and accessible, are frequently targeted by fraudsters.

Common cyber offences now include impersonation of police or government officials (“digital arrest” scams), fraudulent investment and trading schemes, phishing links, OTP

and SIM-swap fraud, loan application extortion, fake job offers, and social media account hacking. Increasingly, offenders are also misusing artificial intelligence tools to create deepfake audio and video messages for extortion and deception. These crimes often operate through organized networks functioning both within the country and from foreign locations, making detection and investigation more complex.

Recent trends indicate that certain regions within India have emerged as operational hotspots, while organized cybercrime networks operating from parts of Southeast Asia are also involved in targeting Indian citizens.

Cybercrime is not merely a technological issue but a social and legal challenge requiring public awareness, responsible digital behaviour, and coordinated institutional response. Preventive awareness is the most effective safeguard. Citizens must understand that cyber offences often succeed not because of complex hacking but because of manipulation, deception, and misplaced trust.

## **B. What is Cybercrime?**

Cybercrime refers to any unlawful act carried out using a computer, mobile device, digital network, or the internet, where technology itself becomes the means, the tool, or the target of the offence. It is often also described as electronic crime or digital crime.

In cybercrime, an offender uses electronic systems to gain unauthorised access, manipulate data, deceive individuals, or disrupt services. The offence may be committed against individuals, organisations, or government institutions. A computer or network may either be used to execute the crime (for example, online fraud) or may itself be attacked (such as hacking or malware attacks).

Cybercriminals typically exploit vulnerabilities in digital platforms to steal personal information, financial details, confidential business data, or official records. They may impersonate legitimate persons, circulate malicious software, extort money, violate privacy, or disable computer systems and essential services.

In simple terms, whenever a crime is committed in cyberspace or through digital technology, it constitutes cybercrime. As modern life increasingly depends on online

communication, banking, e-commerce, and social media, cybercrime has emerged as a serious threat to personal security, economic stability, and public trust.

Thus, cybercrime is not merely a technological issue but a legal and social challenge, requiring awareness, preventive practices, and effective legal enforcement to protect users in the digital environment.

## C. Classification of Cybercrime

The nature of cybercrimes has expanded so much that categorizing them completely is nearly impossible. However, for convenience, some common methods of committing cybercrimes are mentioned below:

1. **Unauthorized Access and Hacking:** Gaining access to a computer, computer system, or network without the permission of the responsible individual or organization. Hacking refers to when a hacker creates a computer program to attack a targeted system and uses it to illegally infiltrate a computer network.
2. **Website Hacking:** Taking forcible control over someone else's website. In such cases, the actual owner loses control over their website and its content.
3. **Pornography:** The display of sexual acts to create arousal, including pornographic websites, digital pornographic magazines, and obscene cartoon videos created using computers.
4. **Child Pornography:** This involves distributing pornographic material to lure children and attempting to engage them in sexual activities or take their nude photos to depict them in sexual acts.

### How it works:

- Criminals use fake identities to lure children/teenagers.
- They interact with children through various chat rooms and gradually build communication with them.
- They befriend children and gain their trust to extract personal information.
- They obtain details of their email and social media accounts to establish further contact.

- Once connected through email or social media accounts, they begin sending obscene content to the child. This gradually reduces the child's hesitation toward such content, making them perceive it as normal.
  - Later, they extract personal information about the child's home and family and lure them outside their home for sexual exploitation or abuse.
5. **Cyber stalking:** Targeting and harassing a victim by following them, making distressing phone calls, sending messages through social media or email, damaging their property, collecting personal information about their family, and spreading false information about the victim to friends and relatives. Cyber-stalkers may also threaten victims to force them into wrongful activities.
  6. **Virus Attack:** A malicious software program designed to infect computers, mobile devices, or data to cause harm.
  7. **Software Piracy:** Illegally duplicating or counterfeiting original software and selling it as a genuine product.
  8. **Phishing:** Cybercriminals send fake emails or messages impersonating a legitimate company or enterprise and direct users to fraudulent websites to deceive them into providing personal information or credentials.
  9. **Illegal Sale of Goods:** Posting advertisements on websites and bulletin boards to sell illegal items.
  10. **Online Gambling:** Providing platforms for online gambling through websites or gaming platforms.
  11. **Email Spoofing:** Sending emails that appear to be from a legitimate source but are actually from a different origin, which can be used for financial fraud or deception.
  12. **Cyber Defamation:** When an individual publishes defamatory content about another person on a website or sends insulting emails to all their friends, damaging their reputation.
  13. **Counterfeiting (Forgery):** Creating fake currency notes, revenue stamps, mark sheets, etc. using computers, printers, and scanners.
  14. **Data Theft:** Stealing electronically stored information that is protected on cloud storage or computers.

15. **Email Bombing:** Sending a large number of emails to a person, causing their email ID to crash.
16. **E-Commerce/Investment Fraud:** Deceiving victims into investing money, applying for loans, or purchasing goods online under false pretences.
17. **Digital Arrest Fraud:** Cybercriminals falsely accuse a person of a crime and stage an online trial, threatening to send them to jail unless they pay a hefty fine.
18. **OTP (One-Time Password) Fraud:** An unknown caller deceives the victim by:
  - Offering fake benefits of a scheme.
  - Threatening to block their mobile SIM.
  - Warning that their bank account, credit card, or debit card will be deactivated. Using other false claims to obtain the OTP sent to the victim's registered mobile number and then transferring money from their account.
19. **Misuse of Photocopies of Identity Cards:** Using copies of identity documents for fraudulent activities.
20. **Credit/Debit Card Skimming:** Using a small device to steal sensitive information from a card's magnetic strip and misusing it for online transactions, creating duplicate cards, or withdrawing money from ATMs.
21. Hacking of Bank Accounts Due to Weak or Common Passwords.
22. Virus Attacks from Downloading Files and Malicious Software from Untrusted Websites.
23. Stealing Personal and Confidential Information by Sending Unsafe Links and Transferring Money Fraudulently.
24. **Deepfake-Related Fraud:** Using artificial intelligence to create manipulated videos or audio to impersonate individuals, often for financial fraud or defamation.
25. **Ransomware Attacks:** Malicious software that encrypts a victim's data, demanding payment for decryption.
26. **AI-Based Cybercrimes:** Using AI-generated content, such as phishing emails or social engineering attacks, to deceive victims.

## **D. Important Provisions in Various Laws Related to Cybercrime**

### **1. Key Provisions of the Information Technology Act, 2000:**

- Tampering with Computer source documents – Section 65
- Computer related offence – Section 66
- Punishment for dishonestly receiving stolen computer resources or communication devices – Section 66B
- Punishment for identity theft – Section 66C
- Punishment for cheating by impersonation using a computer resource or communication device – Section 66D
- Penalty for violation of privacy – Section 66E
- Punishment for cyber terrorism – Section 66F
- Punishment for publishing obscene material electronically – Section 67
- Punishment for publishing material that depicts sexually explicit content – Section 67A
- Punishment for publishing or transmitting child pornography electronically – Section 67B
- Preservation and retention of information by intermediaries – Section 67C
- Provision for unauthorized access to a protected computer – Section 70
- Penalty for misrepresentation of data or information – Section 71
- Punishment for breach of confidentiality and privacy – Section 72
- Penalty for disclosure of information in breach of contract – Section 72A
- Punishment for publishing a false electronic signature certificate – Section 73
- Punishment for publishing information with fraudulent intent – Section 74
- Authority of an inspector-level police officer to investigate these matters – Section 78

### **2. Important Provisions Under the Bharatiya Nyaya Sanhita (BNS), 2023**

- Punishment for sexual harassment – Section 75
- Punishment for voyeurism (spying on someone's private activities) – Section 77

- Punishment for stalking – Section 78
- Punishment for outraging a woman’s modesty through words, gestures, or actions – Section 79
- Punishment for criminal intimidation – Section 351

### **3. Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023**

The BNSS, 2023, replaced the Code of Criminal Procedure and governs procedural aspects of cybercrime investigations, including arrests and evidence collection.

### **4. Digital Personal Data Protection Act (DPDP), 2023**

- The DPDP Act, 2023, governs data privacy and imposes obligations on data fiduciaries to protect personal data, relevant to cybercrimes like data theft and privacy breaches.

#### **Key provisions include:**

- Obligations of data fiduciaries to protect personal data.
- Penalties for data breaches and unauthorized data processing

### **5. Indecent Representation of Women (Prohibition) Act, 1986**

- Sections 3 and 4 define and penalize publications, advertisements, articles, artworks, figures, or any other forms that portray women indecently.

### **6. Protection of Children from Sexual Offences (POCSO) Act, 2012**

- Sections 11 and 12 define and penalize sexual harassment of children.
- Sections 13 and 14 define and penalize the use of children for pornographic purposes.

## **E. Name of the Scheme**

This scheme shall be called "RSLSA (Legal Services for Victims of Cyber Crimes) Scheme, 2026."

## **F. Definitions**

Unless otherwise required by the context in this scheme:

1. 'Act' refers to the Legal Services Authorities Act, 1987 (Act No. 39 of 1987).

2. 'Cybercrime' refers to any online crime committed using the internet or digital devices, including online fraud, theft, espionage, viruses attack and other offenses.
3. 'Legal services' shall have the same meaning as defined under Section 2(c) of the Legal Services Authorities Act, 1987.
4. 'Legal service clinic' refers to a clinic as defined under Regulation 2(g) of the National Legal Services Authority (Legal Services Clinics) Regulations, 2011.
5. 'Legal service institution' refers to the State Legal Services Authority, Supreme Court Legal Services Committee, High Court Legal Services Committee, District Legal Services Authority, or Taluka Legal Services Committee, as applicable.
6. 'Panel Lawyer' refers to those panel lawyers selected under Regulation 8 of the National Legal Services Authority (Free and Competent Legal Services) Regulations, 2010.
7. 'Para-Legal Volunteer' refers to individuals defined as 'Para-Legal Volunteers' (Aadhikar Mitra) under the NALSA Para-Legal Volunteers (Rights Friend) Scheme (Revised) Para-Legal Volunteers Training Module.
8. All other terms and expressions used in this scheme but not specifically defined shall carry the same meaning as assigned to them under the Legal Services Authorities Act, 1987 (Act No. 39 of 1987), the National Legal Services Authority Rules, 1995, or the National Legal Services Authority (Free and Competent Legal Services) Regulations, 2010, as applicable.

## **G. Objectives of the Scheme**

In the present time, the number of cyber-crimes is increasing day by day. Cyber criminals primarily target children, housewives, senior citizens, and illiterate or less educated individuals from marginalized sections of society. These victims are unfamiliar with modern mobile technology and advanced criminal tactics, making them easy targets for cyber-crimes.

The Rajasthan State Legal Services Authority (RSLSA) has observed that victims of cyber-crimes from these sections of society are often unable to speak up about the crimes committed against them. Due to a lack of legal awareness, they do not take any action, resulting in thousands of cyber-crimes occurring daily, causing financial losses and mental distress.

The purpose of this scheme is to:

- Raise awareness about cyber-crimes among vulnerable sections of society.
- Educate them about necessary precautions while using daily digital devices.
- Assist victims in reporting cyber-crimes on appropriate platforms and recovering stolen funds.
- Provide legal aid to victims to resolve challenges faced during legal proceedings.
- Establish coordination among various government departments including the Education Department, Home Department, Information & Technology Department, Women & Child Development Department, Social Justice & Empowerment Department, Police Department, Cyber Cell Pan Rajasthan and organizations working in cyber security to ensure immediate assistance to victims.

Additionally, government and non-government organizations, as well as voluntary institutions, will collaborate to provide necessary aid and support to victims of cyber-crimes.

Employees will be sensitized about cyber-crimes, and victims will be provided with adequate information regarding various national and state-level laws related to cyber-crimes.

## **H. Cyber Redressal Units**

### **SOP for Constitution and Operational mechanism of Cyber Redressal Units**

(STATE & DISTRICT LEVEL)

#### **1. Introduction**

With the rapid growth of digital platforms, cyber offences such as online fraud, identity theft, cyber stalking, child sexual abuse material (CSAM), financial scams, data breaches and misuse of social media have increased significantly. To address these challenges effectively, it is essential to establish dedicated Cyber Units at State and District levels in Rajasthan for prevention, detection, investigation, legal assistance and awareness of cyber crimes.

## 2. Objectives Of Cyber Redressal Unit

The Cyber Redressal Unit shall aims to:

1. Provide free legal aid and assistance to victims of cybercrime who are eligible under Section 12 of the Legal Services Authorities Act, 1987.
2. Facilitate coordination between victims, police cyber cells, Banks/financial institutions.
3. Create legal awareness about cybercrime prevention, victim rights, and remedies available.
4. To strengthen access to justice and enhanced cyber safety for vulnerable and economically weaker sections, especially in cases of small value digital payment frauds. Particular emphasis will be placed on rural, first-time digital-payment users, women, SC/ST, and other disadvantaged groups to prevent financial loss, reduce fear of digital transactions.
5. Monitor and assist in fund recovery through National Cybercrime Reporting Portal (NCRP).
6. Prevent cyber crimes and early intervention.
7. Ensure coordination among stakeholders.
8. Promote cyber safety and digital literacy.

## 3. Constituion of Cyber Redressal Units

### I. Establishment of RSLSA Cyber Redressal Unit

#### ➤ Composition of RSLSA Cyber Redressal Unit:

The RSLSA Cyber Redressal Unit shall Consist of 5 Persons:-

1. A Nodal Officer nominated by Member Secretary, RSLSA
2. One Advocate with expertise in Cyber Laws
3. One Senior Police Officer from State Cyber Crime Wing
4. One Technical Expert (One staff member with knowledge of computers, NCRP portal navigation, and e-filing).
5. One Junior Assistant for documentation and follow-up

➤ **Functioning Of RSLSA Cyber Redressal Unit:**

The RSLSA Cyber Redressal Unit shall function as the Apex Body for planning, coordination, supervision, and monitoring of cyber crime prevention and response mechanisms across the State.

**(a) Capacity Building**

1. Once all DLSA's Cyber Redressal Units are established, RSLSA will conduct orientation training for the all DLSA's Cyber Redressal Unit members, Judicial Officer who have jurisdiction related to Cyber Crime offences, PLVs, Legal Aid Counsel, Panel lawyers, nominated Police personnel from SP office.
2. The training can be conducted physically or through video conferencing.
3. A refresher training will be held at every six month for the unit members.
4. The training programme and curriculum will be determined by the Rajasthan State Legal Services Authority (RSLSA).
5. Government and non-government cyber security experts may be engaged for conducting training programmes.

**(b) Procedural functions of RSLSA Cyber Redressal Units**

1. Receive and process cyber victim applications referred from DLSAs involving complex legal issues.
2. Provide legal aid counsel preferably having knowledge of Cyber related matters.
3. Facilitate the Cyber Crime victim to coordinate with Bank for "put on hold" fund release.
4. The Unit will facilitate Cyber Crime victim to coordinate with concerned Bank/Intermediaries in accordance with applicable guidelines and prescribed procedure by Reserve Bank of India(RBI) and other financial institutions from time to time.
5. The Unit will facilitate the victim to seek the redressal through any venture established by State Government. The Unit functioning under the aegis of the RSLSA shall operate in coordination and collaboration with the corresponding units of the State Government to ensure effective functioning, uniformity in approach, efficient redressal of grievances.

### **(c) Cyber Victim Assistance Helpline**

1. A dedicated Phone number shall be earmarked for the RSLSA Assistance Helpline exclusively for cyber related matters .This number will function as an exclusive cyber helpline, on which specially designated and trained staff will remain available during notified working hours, for the purpose of receiving, processing and facilitating redressal of cyber related grievances
2. All calls received on this cyber helpline will be attended by the State Authority, who will listen to the grievance, collect basic facts, and identify the nature of the cyber offence. Depending on the facts of each case, the state authority shall guide the caller for taking appropriate action under the law.

### **(d) Supervisory & Coordinating Role**

The RSLSA Cyber Unit shall:

1. Supervise the functioning of DLSA Cyber Units
2. Act as the nodal coordination agency between:
  - DLSA Cyber Redressal Units
  - Cyber Police Stations
  - Cyber Cells
  - Bank Institutions.
  - CERT-In (Computer Emergency Response Team) and other National Cyber Agencies
  - CCTNS(Crime and Criminal tracking network and systems)

### **(e) Monitoring Mechanism of RSLSA Cyber Redressal Unit**

1. Monitoring by RSLSA Cyber Redressal Unit
  - Monitor implementation of Cyber legal aid SOPs across all DLSA Units.
  - Review monthly reports from DLSAs and identify systemic issues:

- Monthly report shall contain:
  - Number of complaints received
  - Matters assisted
  - Victim assistance provided
  - Awareness programmes conducted
  - Cases referred to Cyber cells

## 2. Review Meetings

The RSLSA Cyber Redressal Unit shall conduct quarterly meeting on DLSA's Cyber Unit functioning, which will be chaired by Member Secretary, RSLSA and assisted by officer as nominated by Member Secretary, RSLSA with:

- DLSA's Cyber Redressal Units
- Police dealing with Cyber Crime matters
- Cyber cells
- Judicial officers having jurisdiction related to Cyber offences

## **I. Constitution and Function of State Level Cyber Crime Monitoring Committee**

### **(a) Constitution of State level Cyber Crime Monitoring Committee**

RSLSA shall constitute a State Level Cyber Crime Monitoring Committee comprising of:

1. An officer of RSLSA nominated by the Member Secretary, RSLSA
2. One Technical Expert in Cyber Security/Forensics (Special Invitee).
3. Such other members as may be approved by Member Secretary, RSLSA.

### **(b) Functions of the Committee**

The Committee shall perform the following functions:

1. The Committee will recommend the name of advocates for empanelment.
2. To periodically review trends of cyber offences and emerging patterns of cyber crime.

3. To review the functioning of State Cyber Redressal Unit and District Cyber Redressal Units.
4. To ensure effective implementation of Standard Operating Procedures (SOPs) issued by RSLSA and advisories relating to cyber crime matters.
5. The Committee may consider for recommendation of the legal assistance to a victim not falling under the provision of section 12 of Legal Service authority act and may recommend to provide legal assistance through Probono lawyer.
6. To act as a forum for discussing issues faced by DLSAs, panel advocates, PLVs and other stakeholders (Police, Banks, Telecom companies, CCTNS, etc.) in cyber crime and cyber fraud matters, and to suggest solutions.
7. To coordinate with State level stakeholders, including Home Department, Police (DG Cyber), Finance / Banking authorities and IT Department, regarding implementation of Government / RBI guidelines on cyber fraud redressal and compensation schemes.
8. To monitor compliance with the directions of the Hon'ble High Court in cyber crime matters and submit periodic reports.
9. To scrutinize quarterly reports received from the DLSAs' Cyber Redressal Units concerning:
  - Number and nature of cyber complaints received;
  - Legal aid provided to victims;
  - Awareness and outreach activities conducted.

**(c) Meetings and review**

1. The Committee shall hold quarterly meetings to review performance, policy implementation and procedural compliance.
2. The meetings shall ordinarily be held at the RSLSA office or through hybrid / video-conferencing mode, on such date and time as may be fixed.

## **II. Establishment of a DLSAs Cyber Redressal Units**

### **➤ Composition of DLSAs Cyber Redressal Units:**

1. Each District will have a Cyber Redressal Unit, which will be constituted by the Chairman of the District Legal Services Authority who will be serve as the head of the unit and the Secretary of the DLSA will act as the Unit Secretary.
2. A panel advocate experienced in cyber law nominated by Chairman,DLSA
3. Responsible officer placed in Cyber Police Station shall be nominated by the Superintendent of Police on request of Chairman ,DLSA
4. A Public prosecutor/APP nominated by Chairman of DLSA's
5. One System officer posted in district with the knowledge of computers, NCRP navigation, and e-filing will also be member of unit.

### **➤ Functions Of DLSA Cyber Redressal Units**

#### **(a) Awareness and outreach programmes**

- Awareness camps will be organized in collaboration with government and non-government departments to aware and educate the general public, children and women, senior citizen about cyber security and digital arrest.
- “Rajasthan State Legal Services Authority (RSLSA) shall prepare a concise booklet on Cyber matters. The booklet shall be circulated to all District Legal Services Authorities (DLSAs), which will ensure its wider dissemination through PLV's in schools, colleges and other educational institutions through legal literacy clubs, awareness camps, and special drives on cyber safety”
- Cyber-crime awareness will be disseminated through Doordarshan, All India Radio, FM radio, reels, and short videos.
- Many legal aid beneficiaries reside in remote rural areas, it is difficult for them to reach District or Taluka headquarters for legal services, to overcome these challenges, the Legal Services Authority may provide legal services through mobile clinics at the beneficiaries' locations.
- The Rajasthan State Legal Services Authority will also work with the state government to incorporate cybersecurity-related chapters into school curriculum to raise awareness among students.

## **(b) Victim Assistance & Support**

### **1. Front Office:**

The DLSA shall ensure the following procedure:

- To enter details of cyber victims and keep record of cyber victims separately at the front office.
- The front office shall facilitate the applicant or cyber victim and present him/her before Secretaries, DLSA for further course of action.
- Maintain Record details in Cyber Victim Register.

### **2. Scrutiny and Processing of Legal Aid Applications**

- The Secretary, DLSA will get examined the applications from the members of unit constituted under the scheme. Provided if a person is not otherwise, eligible in under section 12 of legal services authority act 1987 the assistance may be provided through Probono lawyers and advocates.
- The Secretary shall ensure to provide legal assistance as soon as possible with due information to victim.
- The progress of each case shall be monitored on a regular basis through monthly status reports to be submitted by the appointed Panel Lawyer.
- The Para Legal Volunteers (PLVs) may reach out to the victim and their family members to provide assistance and support. The PLVs shall coordinate with concerned banks, financial institutions, payment intermediaries, and other relevant authorities to facilitate reimbursement, compensation, or redressal in cyber fraud matters, in accordance with applicable guidelines and procedures.

### **3. National Cybercrime Reporting Portal (NCRP) Assistance:**

- Help victims to register complaints on <https://cybercrime.gov.in>
- Follow up of complaint and facilitate the victim with legal aid throughout prosecution of case, if prayed.

- Maintain the record of cases where assistance is provided.
- Coordinate with District Cyber Redressal Unit for status update.

#### **4. Court assistance:**

- Assist in filing/drafting applications before Trial Courts for release of "put on hold" funds, in cyber fraud cases.

#### **5. CCTNS (Crime and Criminal tracking network and systems)**

- Upon development and operationalization of a specialized portal for filing e-FIRs, the concerned District Legal Services Authorities (DSLAs), in coordination with the police authorities, should take secure access to such FIRs for identifying victim and pattern of Cyber Crime.
- The Secretary may have the access of e-FIR with secured login credentials , provided by the concerned department on request from State level authority.
- The Secretary, DLSA shall ensure strict maintenance of confidentiality, anonymity of victims, particularly in sensitive categories of cases, including those under the Protection of Children from Sexual Offences (POCSO) Act and other child-abuse matters.

#### **(c) Cyber Victim Assistance Helpline**

- DLSA Cyber Redressal Unit shall receive all such complaint relating to Cyber related matters on their regular helpline no., but shall maintain record distinctly. Designated and trained staff will remain available during notified working hours.
- All calls received on cyber helpline will be attended by the district authority, who will listen to the grievance, collect basic facts, and identify the nature of the cyber offence. Depending on the facts of each case, the district authority shall guide the caller for taking appropriate action under the law.

#### **(d) Monitoring and Coordinating Functions:**

- DLSA Cyber Redressal Units shall submit monthly report to RSLSA.
- DLSA's will take follow up with Panel Lawyer for status reports.
- The Chairman, DLSA Cyber Redressal Unit shall convene a coordinating quarterly

meeting involving representatives of the Police/Cyber Cell, Banks and Financial Institutions, Telecom Service Providers, Panel Lawyers, and other relevant stakeholders to review coordination, pendency, bottlenecks, and cyber victims compensation issues. It shall also work closely with banks and financial institutions, including District Lead Bank Officers and nodal officers of major banks, to facilitate communication regarding frozen funds and refund procedures.

- It is expected that learned Judges would sensitize Judicial Officer about such Cyber Crimes in their monthly meetings and may request priority listing of applications pertaining to release of frozen funds.





## **RAJASTHAN STATE LEGAL SERVICES AUTHORITY**

**Rajasthan High Court Campus, Jaipur Bench**

Vidhik Seva Sadan, Vidhik Seva Marg, C-Scheme, Jaipur

Phone No. : 0141-2227481, FAX: 2227602,

Toll Free Help Line 15100/9928900900

Email: [rslsajp@gmail.com](mailto:rslsajp@gmail.com), website: <http://rajasthan.nalsa.gov.in>