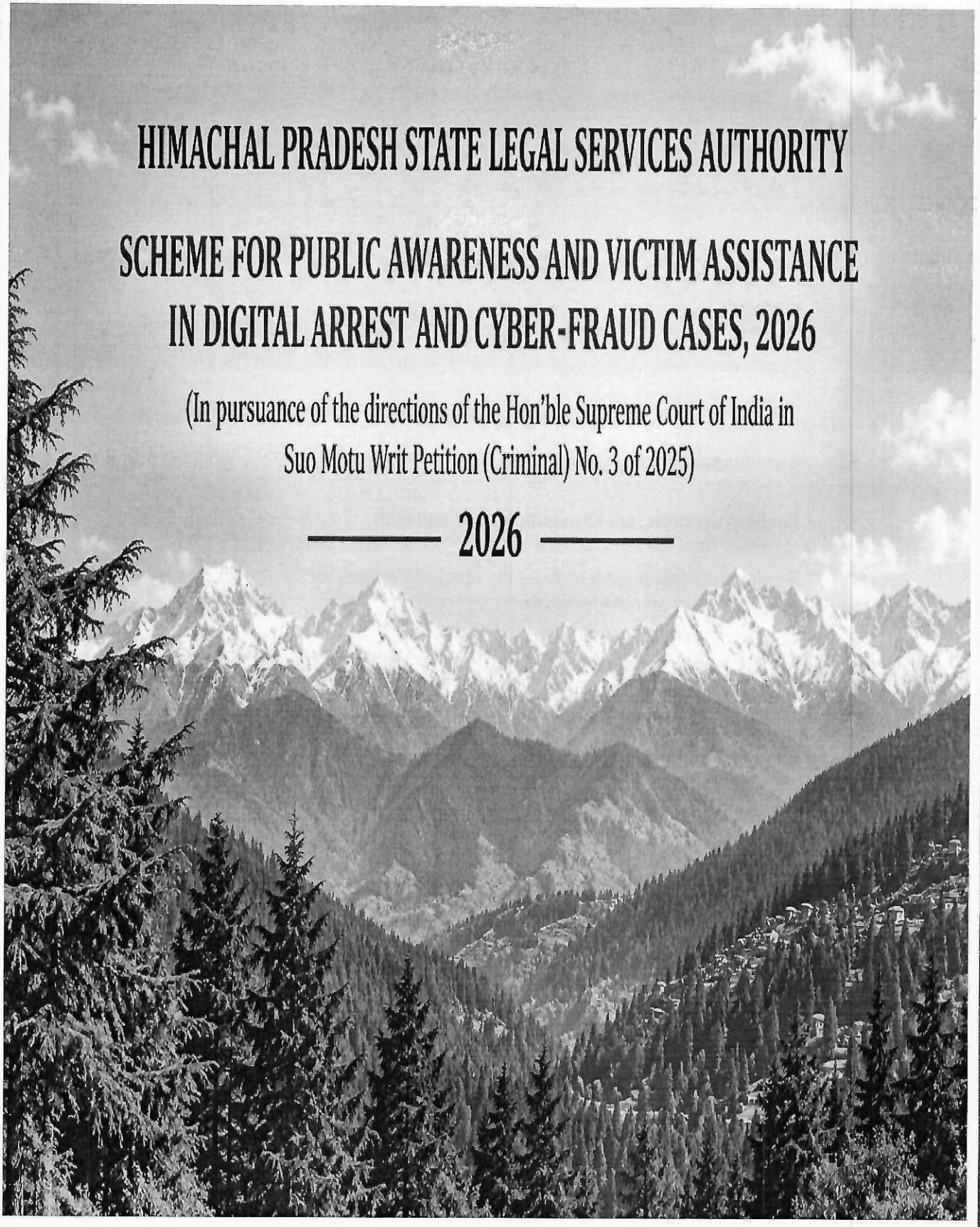


HIMACHAL PRADESH STATE LEGAL SERVICES AUTHORITY

SCHEME FOR PUBLIC AWARENESS AND VICTIM ASSISTANCE IN DIGITAL ARREST AND CYBER-FRAUD CASES, 2026

(In pursuance of the directions of the Hon'ble Supreme Court of India in Suo Motu Writ Petition (Criminal) No. 3 of 2025)

2026

CONTENTS / INDEX

Sr. No.	Particulars	Page No.
1.	Title, Commencement and Applicability	1
2.	Definitions	1-3
3.	Objectives	3
4.	Legal Basis and Alignment with the Directions of the Hon'ble Supreme Court	3-4
5.	Institutional Arrangements	4-5
6.	Public Awareness and Legal Literacy Component	6-7
7.	Victim Assistance and Recovery Facilitation Component	7-9
8.	Capacity Building and Training	9-10
9.	Monitoring, Reporting and Evaluation	10
10.	Funding and Resources	10
11.	Confidentiality, Data Protection and Safeguards	10-11
12.	Miscellaneous	11
13.	Annexure A	12

1. TITLE, COMMENCEMENT AND APPLICABILITY

1.1 This Scheme shall be called the "Himachal Pradesh State Legal Services Authority Digital Arrest and Cyber-Fraud Awareness and Victim Assistance Scheme, 2026" (hereinafter referred to as the "Scheme").

1.2 This Scheme shall come into force with effect from the date of its approval by the Hon'ble Executive Chairman, Himachal Pradesh State Legal Services Authority (HPSLSA).

1.3 The Scheme shall remain in force until modified, superseded or withdrawn by the HPSLSA.

1.4 The Scheme shall apply to all District Legal Services Authorities (DLSAs), Taluka/Sub-Divisional Legal Services Committees and Legal Aid Clinics functioning under the HPSLSA, to the extent applicable.

1.5 The Scheme shall supplement, and shall not prejudice or dilute, any existing scheme, programme or entitlement relating to free legal services, victim compensation, legal awareness, preventive and strategic legal services or assistance to victims of crime.

2. DEFINITIONS

In this Scheme, unless the context otherwise requires:

2.1 **"Act":** "Act" means the Legal Services Authorities Act, 1987, as amended from time to time.

2.2 **"HPSLSA":** "HPSLSA" means the Himachal Pradesh State Legal Services Authority constituted under Section 6 of the Act.

2.3 **"DLSA":** "DLSA" means a District Legal Services Authority constituted under Section 9 of the Act.

2.4 **"Legal Services Institutions":** "Legal Services Institutions" means the Legal Services Institutions constituted or established under the Act and includes such institutions as are recognised or constituted under the Rules, Regulations, Schemes, Standard Operating Procedures (SOPs) and Guidelines made or issued under the Act.

2.5 **"Digital Arrest":** "Digital Arrest" means a fraudulent modus operandi whereby a person is contacted through telephone, video call, messaging application, e-mail or any other electronic means by persons falsely representing themselves to be officials of a court, police authority, enforcement agency, bank, government department or other lawful authority and is: (a) accused of involvement in a fabricated offence, investigation, transaction or unlawful activity; (b) threatened with arrest, detention, prosecution, freezing/sealing of bank accounts or other coercive action; and (c) induced, under fear, intimidation, deception or coercion, to transfer money, share OTPs, passwords, PINs, credentials, personal

information or other sensitive information, without any lawful basis for such purported "digital arrest".

2.6 **"Digital Arrest Scam":** "Digital Arrest Scam" means any fraudulent scheme or modus operandi involving or purporting to involve digital arrest, whether or not monetary loss has actually occurred, and includes attempts, threats and preparatory acts connected therewith.

2.7 **"Cyber-Fraud":** "Cyber-Fraud" means fraud, cheating, impersonation, misrepresentation or unlawful financial loss committed through or facilitated by computers, computer systems, computer networks, communication devices, electronic communication or digital platforms, including, inter alia: (a) impersonation of public officials; (b) phishing and vishing; (c) fraudulent investment or trading schemes; (d) fake loan applications or loan-app fraud; (e) online shopping or marketplace fraud; (f) identity-related fraud; (g) misuse of mule accounts; (h) fraudulent payment or banking transactions; and (i) other cyber-enabled financial frauds.

2.8 **"Victim":** "Victim" means a person who has suffered, or is reasonably likely to suffer, financial loss, deprivation of property, mental distress, reputational harm or other injury as a consequence of a digital arrest scam, cyber-fraud or related cyber-enabled offence. (For the purposes of legal services under this Scheme, eligibility shall be determined in accordance with the provisions of the Act and the applicable rules, regulations and schemes).

2.9 **"Mule Account":** "Mule Account" means a bank account, payment wallet, prepaid payment instrument account, or any other financial account used, knowingly or unknowingly by its holder, for receiving, holding, layering, or transferring proceeds of cyber-fraud or other unlawful activities.

2.10 **"MHA SOP":** "MHA SOP" means the Standard Operating Procedure for NCRP-CFCFRMS, Custody, Restoration of Money and Grievance Redressal, approved on 02.01.2026, as amended, revised or replaced from time to time.

2.11 **"NCRP":** "NCRP" means the National Cyber Crime Reporting Portal established by the Government of India for reporting cybercrime complaints.

2.12 **"CFCFRMS":** "CFCFRMS" means the Citizen Financial Cyber Fraud Reporting and Management System functioning as part of the national cybercrime reporting mechanism.

2.13 **"Panel Lawyer":** "Panel Lawyer" means an advocate duly empanelled by the HCLSC/DLSA/SDLSC for providing legal services under the Act and applicable schemes.

2.14 Words and expressions used but not defined in this Scheme shall, unless the context otherwise requires, have the meanings assigned to them under the Act and

other applicable laws, including the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Information Technology Act, 2000, and other applicable laws, rules and regulations.

3. OBJECTIVES

3.1 **Public Awareness:** To create widespread public awareness regarding: (a) digital arrest scams and their modus operandi; (b) common forms of cyber-enabled financial fraud; (c) warning signs and preventive cybersecurity practices; (d) immediate steps to be taken by a person who receives a suspicious call, message or communication; and (e) available mechanisms for reporting cybercrime, grievance redressal and lawful recovery/restoration of defrauded money.

3.2 **Access to Legal Services:** To facilitate access to free legal services, legal advice and appropriate assistance to eligible victims of digital arrest scams and cyber-fraud, particularly persons belonging to weaker and vulnerable sections.

3.3 **Early Assistance:** To facilitate prompt guidance to victims regarding reporting of cyber-fraud, preservation of evidence and approaching the appropriate police, cybercrime, banking and other authorities.

3.4 **Inter-Agency Coordination:** To facilitate appropriate coordination between DLSAs and concerned police/cybercrime authorities, banks, financial institutions and other stakeholders, without interfering with their statutory or regulatory functions.

3.5 **Capacity Building:** To strengthen the capacity of legal services institutions, panel lawyers, Para-Legal Volunteers and other functionaries to identify, guide and assist victims of cyber-fraud.

3.6 **Preventive and Strategic Legal Services:** To undertake preventive and strategic legal services programmes in accordance with the Act, applicable NALSA schemes and directions issued from time to time.

4. LEGAL BASIS AND ALIGNMENT WITH THE DIRECTIONS OF THE HON'BLE SUPREME COURT

4.1 This Scheme is framed under the Legal Services Authorities Act, 1987, and in furtherance of the statutory mandate of the HPSLSA, DLSAs and SDLSCs to provide free legal services and undertake preventive and strategic legal services programmes.

4.2 The Scheme is intended to facilitate implementation, within the legal-services framework, of the directions and observations issued by the Hon'ble Supreme Court of India in Suo Motu Writ Petition (Criminal) No. 3 of 2025, concerning prevention of digital arrest scams, cybercrime, inter-agency coordination, investigation, grievance redressal and restoration of defrauded money.

4.3 The Scheme shall be implemented in harmony with: (a) the directions/orders of the Hon'ble Supreme Court of India issued from time to time in the aforesaid proceedings; (b) the MHA SOP for NCRP-CFCFRMS, custody, restoration of money and grievance redressal; (c) applicable advisories, directions and instructions issued by the Reserve Bank of India; (d) applicable directions and protocols of the Ministry of Home Affairs, Indian Cyber Crime Coordination Centre (I4C), State Police and Cyber Crime authorities; (e) applicable NALSA schemes, regulations, guidelines and directions; and (f) all other applicable laws, rules and regulations.

4.4 Nothing contained in this Scheme shall be construed as conferring upon the Legal Services Institutions any investigative, adjudicatory, banking, regulatory or law-enforcement power which is not otherwise conferred upon it by law.

5. INSTITUTIONAL ARRANGEMENTS

5.1 State-Level Coordination and Monitoring

5.1.1 The HPSLSA shall oversee, coordinate and monitor the implementation of this Scheme at the State level and may designate an appropriate officer or mechanism for coordinating its implementation, as considered necessary.

5.1.2 The HPSLSA may, wherever necessary, seek the assistance and participation of representatives/nodal officers of the State Police/Cyber Crime Wing, banks, financial institutions, Panel Lawyers and other concerned departments, authorities or agencies for effective implementation of the Scheme.

5.1.3 The State-level coordination shall include:

a) overseeing and reviewing the implementation of the Scheme;

b) facilitating the preparation of State-level action plans and awareness strategies;

c) facilitating the preparation, approval and dissemination of appropriate Information, Education and Communication (IEC) material;

d) reviewing reports and information received from the DLSAs regarding implementation of the Scheme;

e) identifying recurring difficulties and systemic issues in providing legal services and victim assistance;

f) facilitating coordination with concerned departments, authorities, banks, financial institutions and other agencies, wherever necessary and legally permissible; and

g) issuing such operational guidelines or instructions as may be considered necessary for effective implementation of the Scheme, subject to law and the directions of competent authorities.

5.2 District-Level Coordination and Implementation

5.2.1 Each DLSA shall coordinate and monitor the implementation of the Scheme within its jurisdiction under the supervision of the Chairperson, DLSA, through the existing institutional framework of the DLSA, including its Front Office, Sub-Divisional Legal Services Committees, Village Legal Care & Support Centres, Para-Legal Volunteers and Panel Lawyers, as applicable.

5.2.2 The DLSA may seek the assistance of District Police/Cyber Crime authorities, Panel Lawyers, banks, financial institutions and other concerned stakeholders for awareness related activities.

5.2.3 The DLSAs shall:

a) organise and coordinate awareness and outreach programmes relating to cyber crime, digital arrest scams, cyber security and online financial fraud;

b) facilitate access to legal advice and legal aid for eligible persons affected by cyber crime and online financial fraud;

c) guide victims regarding appropriate reporting mechanisms, including the Cyber Crime Helpline No. 1930 and the National Cyber Crime Reporting Portal;

d) maintain appropriate records and requisite data regarding awareness activities, referrals and legal-aid assistance provided under the Scheme;

e) identify recurring difficulties or systemic issues encountered in providing legal services and victim assistance and bring the same to the notice of the HPSLSA; and

f) submit a report to the HPSLSA **once every six months** regarding the implementation of the Scheme, in the prescribed format as **Annexure-A**.

6. PUBLIC AWARENESS AND LEGAL LITERACY COMPONENT

6.1 Target Groups

Priority shall be given to: (a) senior citizens; (b) women and homemakers; (c) students and young persons; (d) persons with limited digital literacy; (e) small traders, shopkeepers and businesspersons; (f) government employees and pensioners; (g) rural and semi-urban populations; and (h) other vulnerable or disadvantaged groups.

6.2 Modes of Awareness

DLSAs shall endeavour to organise, at least quarterly, suitable awareness activities, including: (a) legal awareness camps at courts, tehsil/sub-divisional headquarters, Panchayat Bhawans, community centres and senior citizen forums; (b) awareness programmes in schools, colleges, universities, coaching institutions and other educational institutions; (c) lectures, interactive sessions, debates, essay/poster competitions and street plays; (d) radio talks, television programmes, interviews and local media campaigns; (e) social-media awareness campaigns through official DLSA platforms; (f) dissemination of short videos, infographics and advisories in simple/local languages; (g) distribution of pamphlets, posters, handbooks and other IEC material; and (h) participation in national or State-level cyber-safety awareness campaigns.

6.3 Minimum Awareness Messages

Awareness material should clearly communicate, inter alia, that: (a) there is no lawful concept of "digital arrest" by which a person can be arrested merely through a telephone or video call; (b) citizens should not transfer money merely because a caller claims to be a police officer, judge, government official, bank officer or other authority; (c) citizens should never disclose OTPs, PINs, passwords or other confidential banking credentials to unknown persons; (d) suspicious communications should be independently verified through official channels; (e) in case of financial cyber-fraud, the victim should report the incident immediately through the appropriate national cybercrime reporting mechanism and, where applicable, dial 1930; and (f) relevant evidence such as transaction details, screenshots, call records, messages and other digital evidence should be preserved.

6.4 IEC Material

IEC material shall, wherever appropriate, prominently display: (a) Cyber Crime Helpline No. 1930; (b) the official NCRP web address/QR code; (c) NALSA legal-aid helpline 15100; (d) contact details of the concerned DLSA; and (e) any other helpline or contact number officially notified by the competent authority.

6.5 Content Standards

Awareness material shall be: (a) simple and victim-friendly; (b) preferably available in Hindi and the relevant local language; (c) non-technical and easily understandable; (d) consistent with official advisories and directions; and (e) reviewed and updated periodically to reflect emerging forms of cyber-fraud.

7. VICTIM ASSISTANCE AND RECOVERY FACILITATION COMPONENT

7.1 Eligibility

7.1.1 Any person who is a victim or potential victim of a digital arrest scam or cyber-enabled financial fraud may approach the concerned DLSA for guidance and assistance.

7.1.2 Free legal services under the Act shall be provided to persons satisfying the eligibility requirements prescribed under Section 12 of the Act and other applicable provisions, schemes and regulations.

7.1.3 Priority may be given to senior citizens, women, children, persons with disabilities, persons belonging to weaker sections, persons with limited digital literacy and other vulnerable persons, subject to applicable law.

7.2 Services to be Provided

7.2.1 **Immediate Guidance and Triage:** The victim may be advised to: (a) immediately contact the concerned bank/payment service provider through its official channel; (b) report the financial cyber-fraud through the appropriate cybercrime reporting mechanism and, where applicable, dial 1930; (c) preserve all relevant evidence; (d) inform the police/cybercrime authorities, as appropriate; and (e) avoid further communication or payment to the suspected fraudsters.

7.2.2 **Assistance in Reporting and Documentation:** The DLSA, with the assistance of Panel Lawyers and/or PLVs, may assist the eligible victim in: (a) preparing a concise statement of facts; (b) understanding and completing the NCRP complaint process; (c) organising bank statements and transaction details; (d) preserving screenshots, messages, e-mails, call details and other relevant evidence; and (e) preparing representations/applications to the appropriate authorities.

7.2.3 **Liaison with Banks and law-enforcement Authorities:** Where appropriate, the DLSA, either directly or with the assistance of Panel Lawyers and/or PLVs, may facilitate communication between the victim or the victim's authorised representative and the concerned bank, financial institution or law-enforcement authority in relation to matters including the reporting of fraudulent or unauthorised transactions. The assistance provided under this provision shall remain facilitative in nature and shall not extend to directing or controlling the actions or decisions of any bank, financial institution or law-enforcement authority.

7.2.4 **Recovery/Restoration of Money:** The DLSA, with the assistance of Panel Lawyer, shall assist an eligible victim in pursuing remedies available under applicable law and procedures for custody, restoration or recovery of defrauded money. Any restoration, release, reversal or recovery of money shall remain subject to the orders/directions of the competent authority, court, investigating agency, bank or other authority, as the case may be.

7.2.5 **Legal Representation:** Where the victim is eligible for free legal services, appropriate legal assistance may be provided for: (a) legal advice; (b) representations before competent authorities; (c) applications before courts or tribunals, where legally maintainable; (d) proceedings relating to victim compensation, wherever applicable; and (e) such other legal remedies as may be available under law.

7.3 Cyber-Fraud Legal Aid Clinics

7.3.1 The Front Offices established at the District Courts and Sub-Divisional Courts, as well as the Village Legal Care & Support Centres established at the Gram Panchayat level, shall also function as Cyber-Fraud Legal Aid Clinics for facilitating access to information, legal services and appropriate assistance to persons affected by digital arrest scams and cyber fraud, particularly at the grassroots level.

7.3.2 The Cyber-Fraud Legal Aid Clinics may provide or facilitate:

a) information and guidance regarding the availability of legal advice and legal aid;

b) assistance and guidance in understanding and accessing the National Cyber Crime Reporting Portal (NCRP) and other appropriate reporting mechanisms;

c) information regarding appropriate legal remedies and procedures available to the victim;

d) information regarding victim compensation or other applicable statutory relief, wherever applicable;

e) referral and facilitation of communication with the concerned Police/Cyber Crime authorities, banks, financial institutions or other competent authorities; and

f) such other facilitative assistance as may be permissible under the statutory mandate of the Legal Services Institutions.

7.3.3 Each Cyber-Fraud Legal Aid Clinic shall, wherever practicable, have telephonic access to at least one Panel Lawyer having basic training, knowledge or experience in cyber crime, digital financial fraud or related legal matters, as may be designated by the concerned DLSA.

7.3.4 The Village Legal Care & Support Centres and the PLVs manning such Centres shall actively disseminate information and create awareness among the local community regarding the availability of Cyber-Fraud Legal Aid Clinics and the assistance that may be accessed through them, with particular emphasis on senior citizens, women, students and persons residing in rural, remote and vulnerable areas.

7.3.5 Where a person affected by digital arrest or cyber fraud approaches a Village Legal Care & Support Centre or a PLV for assistance, the PLV may, with the consent of the concerned person, contact the designated Panel Lawyer or the concerned DLSA for appropriate legal guidance and facilitate communication between the victim and the Panel Lawyer, so as to enable the victim to understand and pursue the remedies available under law.

7.3.6 The PLVs shall act only in a facilitative and supportive capacity and shall not provide legal advice in place of a Panel Lawyer, investigate the alleged fraud, communicate or negotiate with suspected fraudsters, access or operate the victim's bank account, or handle any money, OTP, PIN, password, UPI PIN, CVV or other confidential banking credentials of the victim.

7.3.7 The Cyber-Fraud Legal Aid Clinics shall maintain a register recording details of cyber-fraud and digital-arrest cases reported or referred through the Clinic, the assistance/guidance provided, referrals made to the concerned authorities or Panel Lawyer, and awareness activities conducted, in such form and manner as may be prescribed by the HPSLSA or the concerned DLSA from time to time.

8. CAPACITY BUILDING AND TRAINING

8.1 The DLSAs shall endeavour to organise periodic training programmes for: (a) the staff; (b) Panel Lawyers; (c) Para-Legal Volunteers; (d) Legal Aid Clinic functionaries; (e) police officers/officials and other persons associated with implementation of the Scheme.

8.2 Training may cover: (a) digital-arrest scams and emerging cyber-fraud modus operandi; (b) basic cyber-security and evidence preservation; (c) NCRP/ CFCFRMS reporting mechanisms; (d) MHA SOP relating to custody, restoration of money and grievance redressal; (e) applicable banking and regulatory procedures; (f) relevant provisions of criminal law and the Information

Technology Act, 2000; (g) victim compensation and legal-aid mechanisms; and (h) ethical handling and confidentiality of victim information.

8.3 The DLSAs shall develop training modules in consultation with the Police Cyber Crime Wing, banking institutions, relevant experts and other stakeholders.

9. MONITORING, REPORTING AND EVALUATION

9.1 The DLSAs shall maintain basic records and requisite data, such as, (a) number of awareness programmes conducted; (b) approximate number of persons reached; (c) number of victims/persons who approached the DLSA; (d) number of persons provided legal assistance; (e) number of NCRP/reporting-related assistance cases; (f) number of matters in which assistance was provided for pursuing recovery/restoration; (g) broad amount involved in such cases, without disclosing unnecessary personal information; and (h) major difficulties or systemic issues noticed.

9.2 The DLSAs shall include the progress and implementation status of the Scheme in their periodic reports submitted to the HPSLSA, in such manner and at such intervals as may be prescribed by the HPSLSA.

9.3 Reports shall be prepared in such a manner that personally identifiable information of victims is not disclosed except where necessary for lawful purposes.

9.4 The HPSLSA shall monitor and review the implementation of the Scheme from time to time and may issue such directions, guidelines or instructions as may be considered necessary for its effective implementation.

10. FUNDING AND RESOURCES

10.1 Expenditure for implementation of the Scheme shall, subject to availability of funds and applicable financial rules, be met from the funds available to the HPSLSA/DLSAs under appropriate heads.

11. CONFIDENTIALITY, DATA PROTECTION AND SAFEGUARDS

11.1 All information, documents, bank details, identity documents, transaction details, screenshots and other personal information furnished by victims shall be handled with due care and confidentiality.

11.2 Information relating to victims shall be collected and retained only to the extent reasonably necessary for providing legal services, maintaining statutory/ administrative records or complying with lawful requirements.

11.3 Personal information of victims shall not be disclosed to any third party except: (a) with the consent of the victim, where appropriate; (b) where disclosure is necessary for providing legal services; (c) where disclosure is required by law or by a competent authority; or (d) where necessary for preventing or investigating an offence, in accordance with law.

11.4 No DLSA, Panel Lawyer, Para-Legal Volunteer or other functionary shall seek or retain passwords, PINs, OTPs or other authentication credentials of a victim except where specifically authorised by law and strictly necessary for a lawful purpose. As a general rule, victims shall be advised never to disclose such credentials.

11.5 The DLSAs shall take reasonable administrative and technical measures to protect records maintained under the Scheme from unauthorised access, disclosure, alteration or loss.

12. MISCELLANEOUS

12.1 This Scheme is supplementary to existing legal-aid, legal-awareness, preventive and strategic legal-services schemes and victim-compensation schemes.

12.2 Nothing in this Scheme shall be construed as creating an automatic right to recovery, restoration, compensation, reversal or refund of any amount lost through cyber-fraud.

12.3 Any recovery, restoration, release, freezing, debit restriction or other financial action shall be governed by applicable law, judicial orders, regulatory directions, banking procedures and the applicable MHA SOP.

12.4 Assistance provided under this Scheme shall remain confined to legal aid, legal awareness, facilitation and lawful victim assistance.

12.5 The HPSLSA may issue further necessary guidelines, standard operating procedures, reporting formats, IEC material and other instructions from time to time for effective implementation of the Scheme.

12.6 The HPSLSA may modify, amend, supplement or review this Scheme in the light of subsequent directions of the Hon'ble Supreme Court, NALSA, Government of India, State Government or other competent authorities.

12.7 In the event of any inconsistency between this Scheme and any subsequent statutory provision, judicial direction, NALSA guideline or binding Government instruction, the latter shall prevail to the extent of such inconsistency.

H.P. STATE LEGAL SERVICES AUTHORITY

Block No. 22, SDA Complex, Kasumpti, Shimla – 171009 (H.P.)

Telephone: 0177-2623862 | **Fax:** 0177-2626962 |

E-mail: mslegal-hp@nic.in

Website: www.himachalpradesh.nalsa.gov.in

Annexure-A

FORMAT
{Clause 5.2.3(f)}

DISTRICT LEGAL SERVICES AUTHORITY, _____

Sr. No.	Details of Beneficiary/ Target Group	Nature of Assistance/ Service Provided	Brief Details of Case/Matter, if Applicable	Action Taken/ Assistance Provided and Present Status	Date and Venue of Programme/ Activity	Awareness Programme/ Activity Conducted	No. of Beneficiaries/ Participants	Remarks