



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS



**SOP for
Audio-Video Recording under
Bharatiya Nagarik Suraksha
Sanhita (BNSS)**

Bureau of Police Research & Development
Ministry of Home Affairs
Government of India
NH-48, Mahipalpur, New Delhi - 37

DISCLAIMER

This SOP is a suggested guideline for various recordings to be done by using audio-video electronic means under various provisions of the Bhartiya Nagarik Suraksha Sanhita as a reference point for law enforcement agencies (LEAs). This SOP has been prepared after consultations with field practitioners & legal experts. The LEAs are advised to build upon this basic structure according to their peculiar needs & provisions of special and local laws with legal vetting wherever required.

The documents on this subject prepared by Delhi Police, Chandigarh Police, UP Police & Directorate of Forensic Science Services have been referred to while formulating the SOP and credit is duly acknowledged. This is not a legal document.

INDEX

S. no.	Subject	Page no.
	SOP for Audio Visual Recording under BNSS	
1)	Summary of Legal Provisions Related to Videography in New Criminal Laws	4 - 7
2)	SOP at a Glance (Through Flowcharts)	8 - 10
3)	- Note on CERTIFICATION of Audio-Video content to satisfy the mandatory provisions of BSA. - Expert-Related Provisions in New Criminal Laws	11 - 14
4)	SOP In Detail: Policy & Procedures of executing SOP: - Policy - Procedure for processing Scene of Crime - Videography During Search Seizure - Specific Technology Procedures for Recording - Do's & Don'ts while Recording Photographic & Video Evidence - Technological Procedures of Storage & Transportation - Seizure of digital evidence & future of evidence handling	15 - 25
5)	The Schedule – Part A	26
6)	The Schedule – Part B	27

SUMMARY OF LEGAL PROVISIONS RELATED TO VIDEOGRAPHY IN NEW CRIMINAL LAWS				
#	Particulars	Relevant Legal Provision	Legal Mandate	Place of Recording or capturing
1.	Videography recording of the Scene of Crime	Sec 176 Procedure for investigation Sub-section (3) - On receipt of every information relating to the commission of an offence which is made punishable for seven years or more, the officer in charge of a police station shall, from such date, as may be notified within a period of five years by the State Government in this regard, cause the forensics expert to visit the crimes scene to collect forensic evidence in the offence and also cause videography of the process on mobile phone or any other electronic device.	Optional as of now But Mandatory from the date notified by State Govt. within 5 years of 1st July 2024	Scene of Crime
2.	Recording of Search and Seizure	Sec 105- Recording of search and seizure through audio-video electronic means. The process of conducting search of a place or taking possession of any property, article or thing under this Chapter or under section 185, including preparation of the list of all things seized in the course of such search and seizure and signing of such list by witnesses, shall be recorded through any audio-video electronic means preferably mobile phone and the police officer shall without delay forward such recording to	Mandatory	Place of search from where recovery is to be made

		the District Magistrate, Sub-divisional Magistrate or Judicial Magistrate of the first class. Sec 185 (2) - Search by Police officer. A police officer proceeding under sub-section (1), shall, if practicable, conduct the search in person: Provided that the search conducted under this section shall be recorded through audio-video electronic means preferably by mobile phone.		
3.	Information in cognizable cases- FIR For sexual offences where the victim is Mentally or physically disabled	Sec 173-Information in cognizable cases. Provided further that- (a) in the event that the person against whom an offence under section 64, section 65, section 66, section 67, section 68, section 69, section 70, Section 71, section 74, section 75, section 76, section 77, section 78, section 79 or section 124 of the BNS, 2023 is alleged to have been committed or attempted, is temporarily or permanently mentally or physically disabled, then such information shall be recorded by a police officer, at the residence of the person seeking to report such offence or at a convenient place of such person's choice, in the presence of an interpreter or a special educator, as the case may be; b) the recording of such information shall be videographed.	Mandatory	Residence of victim/ any place
4.	Recording of a statement by police for offence of Rape	Sec 176- Procedure for investigation. Provided further that in relation	Optional	Residence of victim/any place of

		to an offence of rape, the recording of statement of the victim shall be conducted at the residence of the victim or in the place of her choice and as far as practicable by a woman police officer in the presence of her parents or guardian or near relatives or social worker of the locality and such statement may also be recorded through any audio-video electronic means including mobile phone.		Choice of victim
5.	Examination of witness by police	Sec 180 - Examination of witnesses by police. (3) The police officer may reduce into writing any statement made to him in the course of an examination under this section; and if he does so, he shall make a separate and true record of the statement of each such person whose statement he records: Provided that statement made under this sub- section may also be recorded by audio-video electronic means. Sec 183(1)- Recording of confessions & statements by magistrates. Sec 183(6)(a)- Provided also that if the person making the statement is temporarily or permanently, mentally or physically disabled, the statement made by the person, with the assistance of an interpreter or a special educator, shall be recorded through audio-video electronic means preferably by mobile phone.	Optional Optional Mandatory	Police station or any other place At the Court of Magistrate

6.	Orders for custody and Disposal of property	Sec 497- Order for custody and disposal of property pending trial in certain cases. (3) The Court or the Magistrate shall cause to be taken the photograph and if necessary, videograph on mobile phone or any electronic media, of the property referred to in sub-section (1).	Direction is for the Court: Photograph mandatory Videography optional	Place of custody of property or as directed by the court.
----	---	---	--	---

Electronic and Digital Eco-System in New Criminal laws

In procedure

In Evidence

In policing

Recording of
Statement
u/s 180 BNSS
and 183(6)(a)

Search & Seizure
by Police u/s 105
& 185 of BNSS

Recording of SOC
By Forensic Team
u/s 176 (3) BNSS

Identification of
persons arrested
u/s 54 BNSS

Trial & proceedings
to be held in
electronic mode
u/s 530 of BNSS

Document
u/s -2(1) (d)
BSA

Evidence u/s -
2 (1)(e) BSA

Electronic/
Digital Record
u/s -61 BSA

Admissibility of
electronic Record u/s-
63 of BSA

Primary
Evidence u/s -
57 BSA

Electronic
Evidence

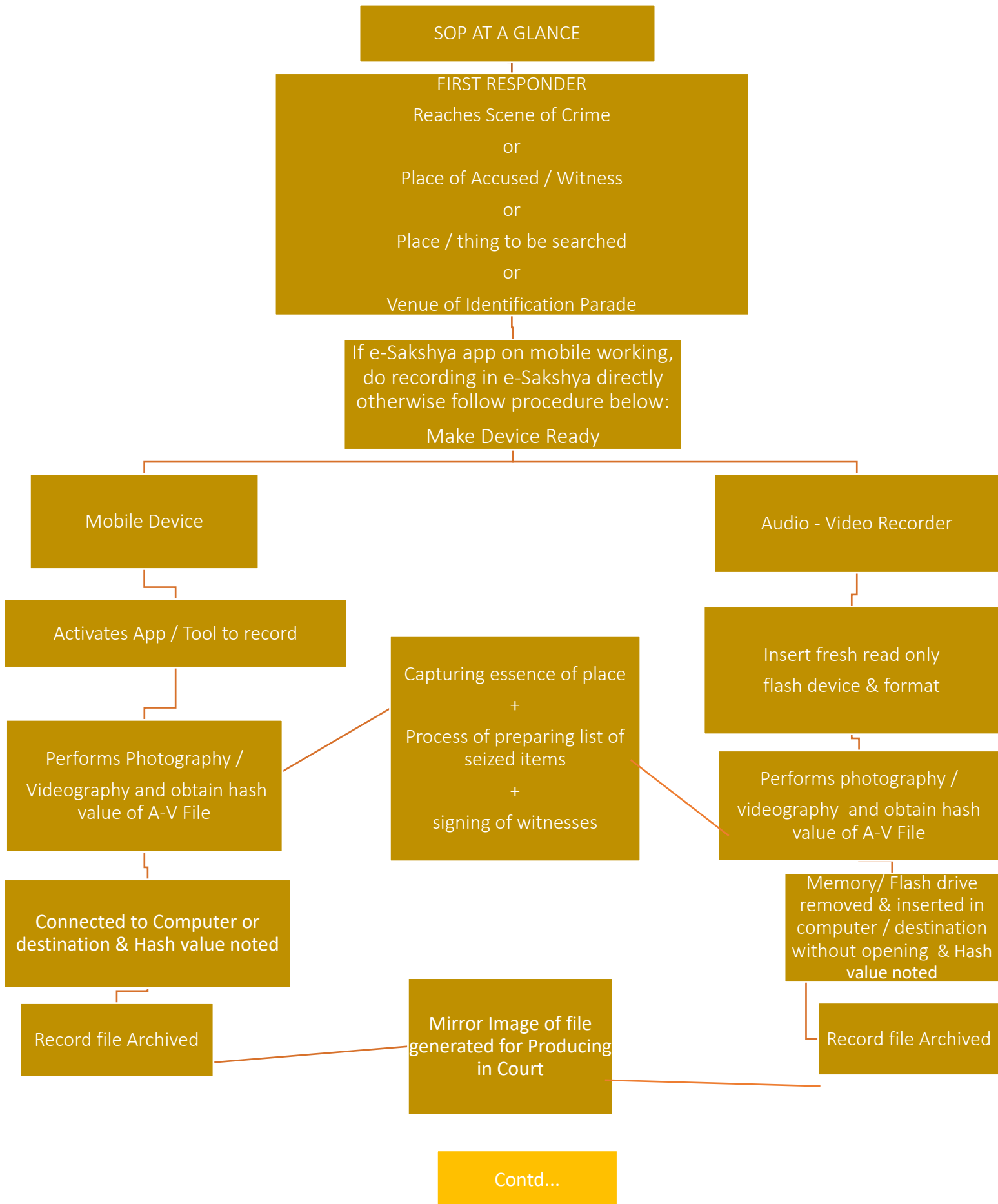
Secondary
Evidence u/s -
58 BSA

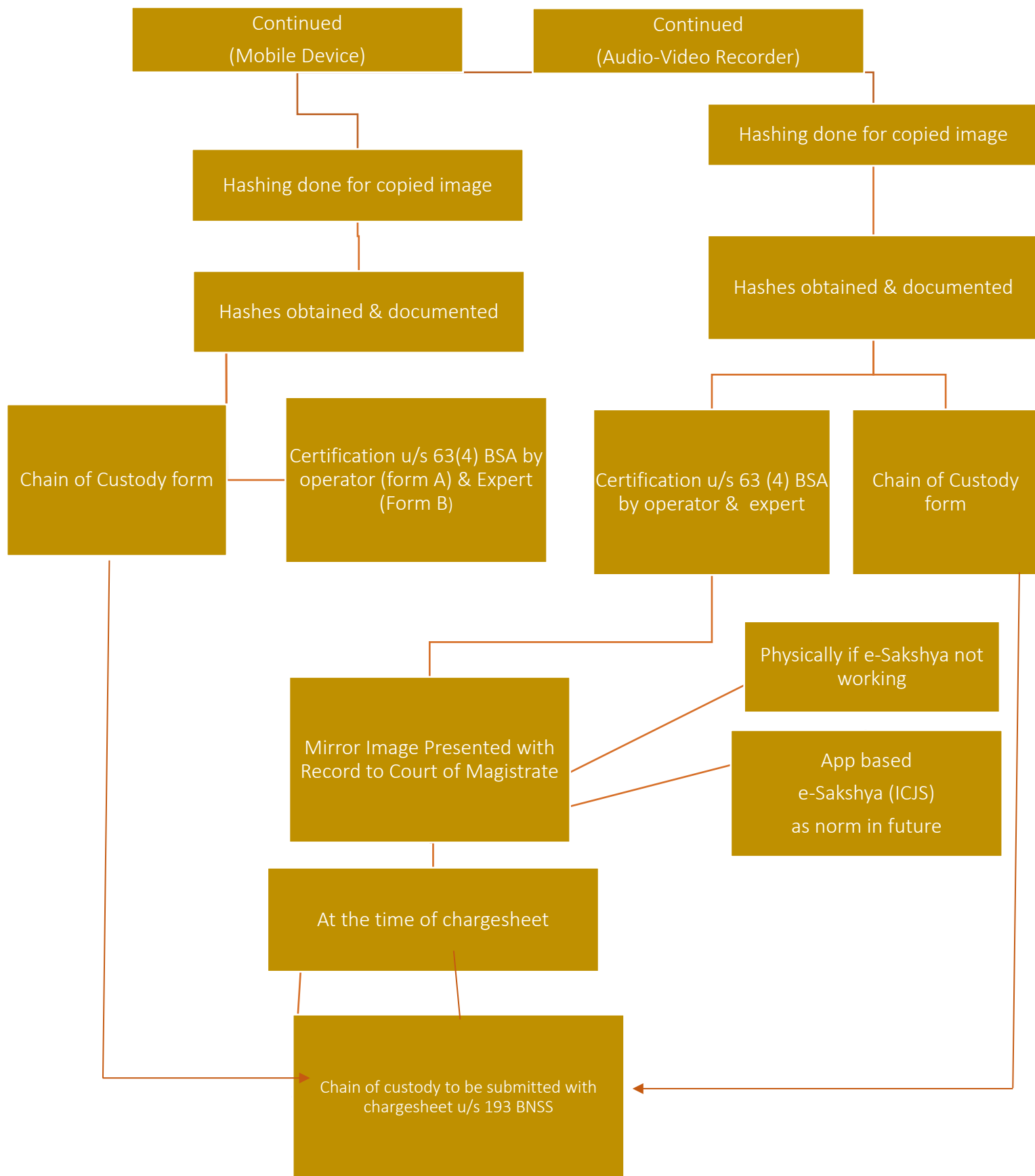
Relevancy
Enhancement of any
Records/ Books

Law Books
u/s 32 BSA

Gazettes
u/s 81 BSA

Presumptions u/s
78 to 93 of BSA





Note on CERTIFICATION of audio-video content as per the mandatory provisions of BSA:

There are two categories of evidence which require certification by experts:

- **First category:** Digital recordings after implementation of new laws:
 - Audio video recording of statements of victim and witnesses, u/s 180 BNSS (Optional)
 - Audio video recording of search and seizure. (Mandatory)
 - Audio video recording of other procedural compliances like identification parade, property disposal. (Optional)
 - Other provisions (Given in the table above)
- **Second category:** Various digital devices are routinely seized during investigations like mobile, social media accounts, emails, computers, CCTV cameras and so on.

Now, the new section 63(4) BSA introduces two new underpinnings viz. “a certificate **shall be** submitted along with the electronic record **at each instance** where it is being submitted” for (a) Identifying the electronic record containing the statement and describing the manner in which it was produced; and (b) Giving such particulars of any device involved in the production of that electronic record.

Thus, now each audio-video recording is part of procedural compliance and investigative compliance and each seizure of relevant digital evidence requires dual certification, part A by the operator (or manager) and part B by an expert.

(Note: The above certifications are required only in case of secondary electronic/ digital evidence and not required where primary recording or storage medium is intended to be used as the evidence).

I. **Owner or Operator/ First Responder/ Manager:**

According to 63(4) (c) BSA: “and purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate)”

Part (A) of the format of the certificate – ‘**to be given by party**’ - as

specified by BSA explicitly refers to the certificate giver of this part to be the owner/ handler or operator/first responder/manager. However, the sequence of custody form should mention the change of hands and the reasons thereof.

Similarly, in the case of the seizure of digital evidence, **‘the party’** or giver of certificate of Part -A of 63(4)(c) can be the owner/operator/handler or manager or person in-charge of communication /computer device in contention.

II. **Expert**

Part -B of the certificate of section 63(4)(c) BSA is to be given by an **expert**. Whereas, the part A certificate, which has to be provided by ‘the party’, flows from the old Indian Evidence Act as such, this ‘*expert*’ added for first time in this new law, appears, from the legislative intent, to be an expert, who can issue part -B of the said certificate and make this admissible in the court of law. And hence for the limited purpose of collection of secondary evidence and for this secondary evidence to become admissible.

Expert-Related Provisions in New Criminal Laws:

I. Section 39 of BSA:

39(1) When the Court has to form an opinion upon a point of foreign law or of science or art, or any other field, or as to identity of handwriting or finger impressions, the opinions upon that point of persons specially skilled in such foreign law, science or art, or any other field, or in questions as to identity of handwriting or finger impressions are relevant facts and such persons are called **experts**.

Illustrations.

- (a) The question is, whether the death of A was caused by poison. The opinions of experts as to the symptoms produced by the poison by which A is supposed to have died, are relevant.
- (b) The question is, whether A, at the time of doing a certain act, was, by reason of unsoundness of mind, incapable of knowing the nature of the act, or that he was doing what was either wrong or contrary to law. The opinions of experts upon the question whether the symptoms exhibited by A commonly show unsoundness of mind, and whether such unsoundness of mind usually renders persons

incapable of knowing the nature of the acts which they do, or of knowing that what they do is either wrong or contrary to law, are relevant.

- (c) The question is whether a certain document was written by A. Another document is produced which is proved or admitted to have been written by A. The opinions of experts on the question whether the two documents were written by the same person or by different persons, are relevant.

(2) When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000, is a relevant fact.

Explanation — For the purposes of this sub-section, an Examiner of Electronic Evidence shall be an **expert**.

II. Section 63(4) (c) of BSA

In any proceeding where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things shall be submitted along with the electronic record at each instance where it is being submitted for admission, namely: —

- (a) identifying the electronic record containing the statement and describing the manner in which it was produced.
- (b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer, or a communication device referred to in clauses (a) to (e) of sub-section (3);
- (c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,

and purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate) and an **expert** shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it in the certificate specified in the Schedule.

III. Section 329 BNSS: Reports of certain Government scientific experts.

BNSS also has a provision which defines Government Scientific Experts. This provision is also relevant while dealing with evidence.

329. (1) Any document purporting to be a report under the hand of a Government scientific expert to whom this section applies, upon any matter or thing duly submitted to him for examination or analysis and report in the course of any proceeding under this Sanhita, may be used as evidence in any inquiry, trial or other proceeding under this Sanhita.

(2) The Court may, if it thinks fit, summon and examine any such **expert** as to the subject matter of his report.

(3) Where any such expert is summoned by a Court, and he is unable to attend personally, he may, unless the Court has expressly directed him to appear personally, depute any responsible officer working with him to attend the Court, if such officer is conversant with the facts of the case and can satisfactorily depose in Court on his behalf.

(4) This section applies to the following Government scientific experts, namely: -

Apart from (a) to (f) which are sector-specific,

(g) ***any other scientific expert specified or certified, by notification, by the State Government or the Central Government for this purpose.***

Note: LEAs may be required to approach their State government or Central government as the case may be, for declaring any competent person as government scientific experts, including experts from State/ Central FSL or National Forensic Science University (NFSU) wherever available, under the provisions of section 329 (4)(g) BNSS to fulfil the requirements of the experts required to provide Part B of the certificate under 63 (4)(c) of BSA.

POLICY & PROCEDURES OF EXECUTING SOP

1. POLICY

The Photographs and videography are universally accepted best practices and are critical for the appreciation of the scene of crime and evidence by the Hon'ble trial court. Therefore, the recording of the scene of crime via videography and photography preferably, be done by the first responder itself. Specific and expert photography for better appreciation of the evidence can be done by forensic experts.

2. PROCEDURE FOR PROCESSING SCENE OF CRIME

Basics of Audio-visual Recordings

Preparation:

- Verify that the audio-video recording equipment is operational.
- Inform all parties present about the recording process.
- Use a tripod or stabilizer to prevent shaky footage, wherever available.
- Limit the presence on the scene of crime and preferably none other than the mandatory required people/ witnesses should be present in that area during the process of videography.
- For recording the statement of the subject/witness set up a close-up frame.
- The quality of videography/photography should be given proper attention. If one anticipates a low light environment, carry a torch/additional light source with yourself.

3. VIDEOGRAPHY DURING SEARCH SEIZURE

- **Avoid talking while shooting the video** and capturing the photographs at the crime scene.
- Ensure that **the audio recorder is off** & also turn off mic devices available with the officials present at the crime scene. If recording on a mobile phone, preferably put it in airplane mode to avoid disturbance from incoming calls.
- Begin recording while entering the premises.

- Clearly announce the commencement of the search and seizure operation.
- Include a clear introduction with the date, time, location, case details, and warrant details. As far as possible, the latitude- longitude and time of recording should be recorded along with the video.
- Capture a 360-degree view to document its initial condition.
- Document the search process methodically, covering each room or area in sequence.
- Focus on capturing the entire search process, including a detailed walkthrough of the area being searched.
- Capture close-ups of seized items, showing their condition and any identifying marks.
- Clearly narrate the discovery and seizure of items, ensuring they are visible in the recording.
- Record the preparation and signing of the seizure list by witnesses.
- Ensure continuous recording from start to finish without unnecessary interruptions.
- End the recording with a summary of the search seizure operation.

Post-Recording

- Review the recording for accuracy and completeness.
- Securely store and back up the recording.
- Label the recording with the date, time, location, case details, and a brief description of the content.

4. SPECIFIC TECHNOLOGICAL PROCEDURES OF RECORDING

1. Only departmentally approved and issued recording devices should be used for official criminal investigation purposes.
2. Till appropriate recording devices or standalone devices are procured and made available to field investigation/responder units, for all practical purposes, mobile/smartphones are going to be the preferred medium of recording, due to practicality and because the statute specifically encourages it. As per recently circulated ICJS Guidelines of NCRB, the specification for Mobile's camera is a minimum of 3.0

megapixels (3.2 MP gross), for front camera & 8 megapixel for back camera with 300ppi or higher. Forensic experts using recording devices follow specs circulated by DFFS.

3. At the beginning of each tour of duty, it shall be the responsibility of the officer to ensure that-
 - a. The issued recording device is in proper working condition,
 - b. The recording device has a clean image memory card (wherever applicable) and the camera or mobile battery is fully charged. The officer should also have a 90-degree evidence ruler which gives white, grey and black vertical and horizontal planes to be used when taking close-up photographs/videos of injuries.
 - c. If using a digital camera, the date stamp is correctly set and the date stamp is set so that it will not be printed on the digital images.
 - d. The camera in mobile/ recording device is set at “automatic” for exposure, flash and focus. The storage control should be set to “best quality.”
4. In taking digital photographs/videos, the officer should take several photographs/videos. When taking photographs of injuries, the officer should have the camera at a 90-degree angle to the injury.
 - a. The photographs/video should include the following:
 - (1) A photograph/video of the general scene or if an individual, a full frame photograph/video of the person.
 - (2) A photograph/video showing the relationship of the injury to the subject’s body, and
 - (3) A closeup photograph/video of the injury, with and without the evidence ruler in the photograph/video.
 - b. If recording using a digital camera, the officer taking digital photographs at the crime scene should view the photographs on the camera’s LCD view screen to determine if the photographs effectively document a victim’s injury or the scene of a crime.
 - c. The officer at the scene of the crime should not delete any digital images which are photographically faulty. Digital images that are relevant for investigative or trial purposes can be printed later.
 - d. The digital photographs/video shall not be viewed with any device that would enable editing of the digital images, such as a memory card reader or a computer.
 - e. The officer should record the camera’s/audio video recorder's assigned

numbers for the images taken for a particular crime scene or case.

- f. The officer should note in the officer's incident report that photographs/ Video had been taken of the victim and the scene.
- g. The process of preparing a seizure memo and signing the same by the witnesses and concerned person also should be video-graphed. Details of the camera, date/time and description of storage media i.e. memory card should be mentioned in the seizure memo which matches with the details generated by the camera.

5. DO's & DON'Ts WHILE RECORDING PHOTOGRAPHIC & VIDEO EVIDENCE

- 1. Use the safe route when moving through the scene, and avoid disturbing the scene of crime.
- 2. It is important to calibrate the time and location of the camera before starting recording.
- 3. The whole episode of recording must be without any break. Also, all team members of the first responder team or forensic team should maintain silence during videography and avoid any chatter or loose talk which could be then used by the defence to counter the investigative sanctity. The same is also expected of witnesses present there.
- 4. Ensure proper lighting arrangements while conducting a search.
 - a. Take photographs and video of the crime scene before and after the alteration.
 - b. Take a complete set of pictures including aerial, long-range, mid-range and close-ups.
 - c. The photographs and video should include entry and exit routes, victims and evidence as far as possible.
 - d. Take photographs and video of crime scene objects such as blood stains, fingerprints or footprints as soon as possible.
 - e. Take photographs and video from the exterior to the interior of the crime scene and from general to the specific focus.
 - f. Close-up photography and recording are preferred when taking footprints, fingerprints, shoeprints, tyre tracks, injuries etc.

5. Take photographs and video with scale when appropriate.
6. To take spare blank memory cards.
7. If the search is to be prolonged than the anticipated capacity of one memory card, then there should be two audio-video recorders so that continuity may be maintained by recording the scene of the crime. Also, if the change of memory card is being done on the first recorder, it may be captured with another spare device and that recording also shall be preserved with the main memory card.
8. It is to be taken on record that the memory card was blank before any recording.
9. The process of recovery of evidence with closeup videography revealing the identifiable details of the recovered evidence should be done.
10. Don't submit unclear photographs and recordings to the court of law.
11. Ensure the admissibility of the digital evidence, by following the procedures demanded by law including the certificate under Sec. 63(4)(c) of BSA.
12. Don't forget to mention the hash value of the individual photograph and video in the case diary.

6. TECHNOLOGICAL PROCEDURES OF STORAGE, CERTIFICATION & TRANSPORTATION

I. Procedure for issuance of Certificate of Part A of Section 63(4) (c)

At the conclusion of the officer's tour of duty, the officer shall:

- a) In case of audio-video recording(s) done on a Mobile phone, (wherein it is stored on mobile's internal memory or on memory card), the police officer/ operator, should apply hashing software through app/web-based tool on the mobile itself and generate the hash value, note it down and transfer the recording to the expert in the police station, on to the local designated desktop - via Cable or Bluetooth or other default file transfer methods. Police officer shall produce a Part-A certificate of section 63(4)(c) to the officer in charge of the police station/investigation unit as his part of execution is complete.

- b) If the police officer/ operator does not have the hashing tool or app or is not confident of hashing techniques, he/she can take the help of the designated expert of the police station. Mention this entire process in the chain of custody form along with the name of the hashing software used. Also, mention whether the hashing was done by the police officer/operator independently or with the help of an expert in his/her presence. It is also advisable to take screenshots of the hash value in order to avoid human errors.

[Note -The expert, before transferring the Audio Video recording to the computer system, should ensure they have any antivirus/anti-malware system running on the computer system]

- c) In case a digital camera/ recording device with a detachable memory card is used, the officer/operator shall hand over the standalone recording device/ camera's memory card to an expert in the headquarters/police station by placing the memory card in an evidence envelope with identifying case information and sealed. This sealed envelope will then be delivered to the expert.

[Note: This is a best practice which is suggested to be followed since this will make the chain of custody more foolproof, and seal applier & seal opener shall be privy to the seal's characteristic & the same should be adduced with signatures in the chain of custody form]

- d). If a memory card or a standalone device has been handed over to the expert, in a sealed envelope, the expert will open the envelop and and calculate the hash value of the recordings from the storage device before copying it to the desktop **in the presence of the police officer/operator**. The police officer shall, after noting the hash values in his certificate, produce a Part-A certificate of section 63(4)(c) to the officer in charge of the police station mentioning the hashing software and the fact that the hashing was done by the police officer/operator with the help of expert in his/her presence. The expert should ensure he/she should not open/rename the recordings/images before hashing (this means, the digital audio-visual recording(s) shall not be viewed with any device/software that would enable editing of the digital audio-visual recording(s).

II. Procedure for issuance of Certificate of Part B of Section 63(4) (c)

a). The expert will now transfer the recording obtained from the first responder/ police officer to the designated computer/device. The digital audio-visual recording(s) transferred on the hard disc of the desktop will become the “**master negative.**” The master negative Hard Disk or storage device shall serve as the permanent record because it should not be altered once written/stored.

- The downloaded file will be named in a manner so that the relevant metadata of FIR Number, police station, date and serial number of the video related to the offence is captured therein. The standard format will be

FIR No_.....dd/mm/yy_.....S No.....

- The police officer will make an entry in the general diary regarding the downloading of the video wherein the file name (as explained in (iii) above) will be linked to the FIR number, Police Officer ID, Date and Time of recording, Latitude-Longitude and any other remarks, if any.
 - After ensuring the above, the AV recording can then be deleted from the police officer’s smartphone or audio-video recorder, making space for more recordings to be made in the future.
- b). Having copied the image, final **hashing** should be done at this stage. That is, he will then take another hash value for the respective recording(s)/images(s) and match the hash values with those of the primary recording and ensure both the hash values are the same, in order to preserve its integrity as potential evidence. **Transfers should be depicted in the chain of custody forms with the expert signing it duly.**
- c). The files on the master negative hard disk or storage devices should be copied, **without opening**, onto another pen drive or storage device which becomes the ‘*working record*’, the “**negative duplicate or mirror image.**” **This mirror image with both certificates A & B has to be supplied to the magistrate.**
- d). Once the master negative hard disk or storage device has been created, it shall not be removed from the custody of the appropriate

department or officer. If the storage device is to be reviewed beyond the custody of the appropriate agent, a new storage device should be made from the negative duplicate hard disc or storage device, such as for the investigating officer, prosecutor, defence attorney, etc.

- e). Any enhancement of digital image files should be documented by the expert/evidence specialist and recorded on a separate pen drive or storage device.
- f). The process of obtaining certificates required under 63(4) (c) Part-B should be started and completed by the expert and handed over to the officer-in-charge.

[Summary of Hashing: It is being repeated for the sake of clarity that Hashing is done of primary evidence i.e. original media as well as copied/mirrored copy of the media to prove that both have the same data by matching the hash value. In summary, the operator or first responder (police officer) either uses a hashing tool/app to generate the hash value and hands it over to the expert along with the certificate or takes the help of the expert to generate the hash value of primary evidence and transfers the recording in mobile to the dedicated computer. The expert after transferring the primary evidence to the dedicated hard drive/device again applies the hashing tool to create a hash value for the copied image and document both hash values. **Transfers should be depicted in the chain of custody forms with the responder & evidence expert signing duly.]**

Different hashing algorithms are as follows:

- MD5 (Message Digest 5) - once widely used but now considered less secure due to potential collisions.
- SHA-1 (Secure Hash Algorithm 1) also facing security concerns and phasing out.
- SHA-2 family (SHA-256, SHA-384, SHA-512)- widely used, secure, and recommended for most applications.
- SHA-3 (Secure Hash Algorithm 3) - newer, more efficient, and designed for future security needs.

There are some open-source tools available for hashing which may be accessed, or appropriate tools be procured for this purpose.

When seizing digital evidence/ device simultaneously as part of investigative compliance/ necessity, along with videography, **hashing should be done preferably through write blocking devices to make it alter proof or any accidental data tampering due to mishandling.** (Write blockers help in Hashing for files and imaging for the entire storage device and help prevent modification of the original data, preserving its integrity as potential evidence). Blockers are required during the seizure of digital storage devices and could be used once they are made available to the field Investigation units.

III. Procedure For Back-up

The master negative hard disk or storage devices should be placed in a secured location or on a designated desktop and not become part of the investigative case files. **The expert will then create a backup copy of the master negative and store it as a backup.**

As an ideal case, till fully integrated with [e-Sakshya](#), an interim policy should be adopted by states/organisations to timely transfer of the stored data which is master negative and needs storage for a considerable time, maybe decades. The backup of master-negative should be stored, in data centres or on the cloud, as per their policy, at another location which can be used in case of any natural disaster or calamitous occurrence.

IV. Transport of audio-video recordings:

- Section 105 BNSS mandates that the record of audio-video recording should be produced to the concerned court as soon as it is done.
- Courts will have to be provided with video files along with certification & chain of custody for which a mirror file from the destination computer where recorded files have been downloaded/archived and hashed would be supplied to the court in a storage device like a pen drive etc. All originals should therefore be stored in a designated/partitioned hard drive, on a desktop of a police station in a separate file which is not touched by anyone once it is hashed. IOs/Responders can make a

copy of files and store them in more accessible parts of computers. **Transfers should be depicted in the chain of custody forms with the responder & evidence expert signing them duly.**

- The expert, data manager, or designated officer at the Police Station **will transfer the mirror images** (preferably all recorded in the last 24 hours) **in a secure storage device to the designated desktop of the Magistrate** along with memos and chain of custody forms.

V. **Sequence of custody** of electronic evidence is crucial. A clear record of the sequence of custody should be kept in writing for each package till it is handed over to the concerned magistrate for perusal or to the FSL for forensic examination.

Document the sequence of custody-

- Name and signature of each person, including internal staff, who take possession of or transport the evidence.
- Date of transfer.
- Evidence labelled or serial number.

The notes and reports should be done in chronological order and should include no opinions, no analysis or no conclusions but just facts.

7. SEIZURE OF DIGITAL EVIDENCE & FUTURE OF EVIDENCE HANDLING

The basic premise of seizing digital evidence is that **'If forensic tools are available, create a forensic image copy. Otherwise, send the device to the nearest forensic lab'**. Now the seizure of digital evidence & audio-visual recording will invariably be going simultaneously. So, two sets of certifications, each with part - A and part - B, will be going on simultaneously sometimes, for recording & seizure.

Since the overall demand for experts is very high for practical implementation there will always be gaps, NIC has already developed software to capture audio/video and generate hash reports with time stamps ([e-Sakshya](#)). LEAs should consider adopting this application for the sake of uniformity.

Note

A case captioned ***Ram Ramaswamy v Union of India*** is pending before the Hon'ble Supreme Court of India urging the Court to pass guidelines regulating the seizure of electronic devices. Since the Government has formed a committee on this issue, which will be coming up with revised guidelines, Hon'ble Supreme Court has directed in the interim order that: **"...for the time being at least the CBI manual will be followed by all the Central Government agencies."**

Hence while using this SOP on Audio-Video Recording, for concurrent seizure of digital evidence, central agencies or even state agencies can follow **the CBI manual** after accounting for the changes in the sections as per the New Criminal Laws.

THE SCHEDULE

[See section 63(4)(c)]

CERTIFICATE

PART A

(To be filled by the Party)

I, _____ (Name), Son/daughter/spouse of _____
residing/employed at _____ do hereby solemnly affirm and
sincerely state and submit as follows:—

I have produced electronic record/output of the digital record taken from the following
device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: _____

Make & Model: _____ Color: _____

Serial Number: _____

IMEI/UIN/UID/MAC/Cloud ID _____ (as applicable)

and any other relevant information, if any, about the device/digital record ____ (specify).

The digital device or the digital record source was under the lawful control for regularly
creating, storing or processing information for the purposes of carrying out regular
activities and during this period, the computer or the communication device was working
properly and the relevant information was regularly fed into the computer during the
ordinary course of business. If the computer/digital device at any point of time was not
working properly or out of operation, then it has not affected the electronic/digital
record or its accuracy. The digital device or the source of the digital record is:—

Owned ☐ Maintained ☐ Managed ☐ Operated ☐

by me (select as applicable).

I state that the HASH value/s of the electronic/digital record/s is _____,
obtained through the following algorithm:—

☐ SHA1:

☐ SHA256:

☐ MD5:

☐ Other _____ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

(Name and signature)

Date (DD/MM/YYYY): _____

Time (IST): _____ hours (In 24 hours format)

Place: _____

PART B

(To be filled by the Expert)

I, _____ (Name), Son/daughter/spouse of _____
residing/employed at _____ do hereby solemnly affirm and
sincerely state and submit as follows:—

The produced electronic record/output of the digital record are obtained from the following
device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: _____

Make & Model: _____ Color: _____

Serial Number: _____

IMEI/UIN/UID/MAC/Cloud ID _____ (as applicable)

and any other relevant information, if any, about the device/digital record _____ (specify).

I state that the HASH value/s of the electronic/digital record/s is _____,
obtained through the following algorithm:—

☐ SHA1:

☐ SHA256:

☐ MD5:

☐ Other _____ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

(Name, designation and signature)

Date (DD/MM/YYYY): _____

Time (IST): _____ hours (In 24 hours format)

Place: _____



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS



NCRB Mobile App “NCRB Sankalan of Criminal Laws”

NCRB has launched a Mobile App “NCRB Sankalan of criminal Laws”. This App is compilation of new criminal laws namely Bharatiya Nayaya Sanhita, Bharatiya Nagarik Suraksha Sanhita and Bharatiya Sakshya Adhiniyam. It is available on Googleplay store as well as Apple App store. This App is useful for General Public, Court Officers, Advocates, Law Students as well as for Police Officers in enhancing their knowledge about the New Criminal Laws. This App serves as a comprehensive guide providing complete information about the new criminal laws at one place. It provides an Index linking all Chapters and Sections of the new laws and a corresponding chart for section wise comparison between old and new laws with a search and linking facility for quick information retrieval. The App is designed to work in offline mode also in absence of connectivity. With its user-friendly design, comprehensive content, and innovative features, the app empower susers to learn the new laws effectively.



<https://ncrb.gov.in/uploads/SankalanPortal/Index.html>

@BprdIndia officialBPRDIndia bprdindia @bureauofpoliceresearchdeve7705 bprd.nic.in

New Criminal Laws courses available on iGOT Karmayogi Platform



Overview of BNSS, 2023 for Field Practitioners



Overview of Bharatiya Nyaya Sanhita, 2023 for Field Practitioners



Overview of Bharatiya Sakshya Adhiniyam, 2023 for Field Practitioners