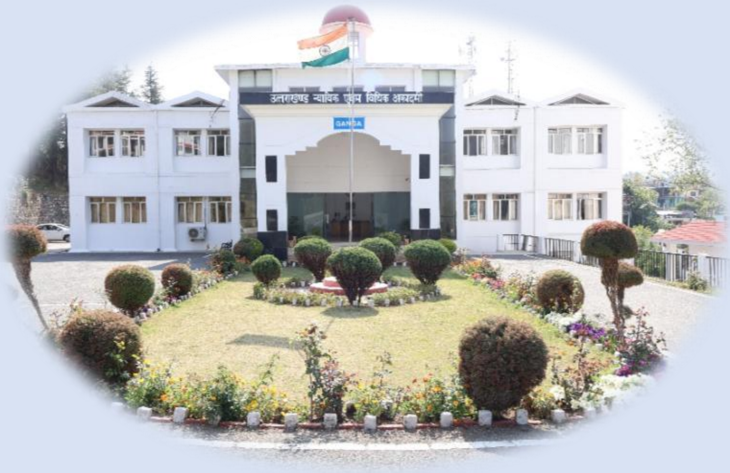

STUDY MATERIAL
ON
TRAINING PROGRAMME FOR THE OFFICERS
OF
SECURITIES AND EXCHANGE BOARD OF INDIA (SEBI)
&
JUDGMENT OF HON'BLE SUPREME COURT
&
VARIOUS HIGH COURTS
(FROM 15.09.206 TO 17.09.2026)

PREPARED BY

UTTARAKHAND JUDICIAL AND LEGAL ACADEMY, BHOWALI

STUDY MATERIAL ON INVESTIGATION, BAIL, CYBER LAWS, DISPOSAL OF PROPERTY COGNIZANCE ON COMPLAINT AND PROCEDURE TO BE ADOPTED & SEARCH AND SEIZURE ETC
&
JUDGMENT OF HON'BLE SUPREME COURT& VARIOUS HIGH COURTS

SL. NO.	TITLE, CITATION	LAW POINT
INVESTIGATION		
1.	**State of Uttar Pradesh v. Bhagwant Kishore Joshi, (1964) 3 SCR 71**	**AN INVESTIGATOR IS THE KINGPIN OF CRIMINAL JUSTICE DELIVERY SYSTEM** "17. What is investigation is not defined in the Code of Criminal Procedure; but in H.N. Rishbud and Inder Singh v. State of Delhi [(1955) 1 SCR 1150, 1157-58] this Court has described, the procedure, for investigation as follows: "Thus, under the Code investigation consists generally of the following steps, (1) Proceeding to the spot, (2) Ascertainment of the facts and circumstances of the case, (3) Discovery and arrest of the suspected offender, (4) Collection of evidence relating to the commission of the offence which may consist of (a) the examination of various persons (including the accused) and the reduction of their statements into writing, if the officer thinks fit, (b) the search of places of seizure of things considered necessary for the investigation and to be produced at the trial, and (5) formation of the opinion as to whether on the material collected there is a case to place the accused before a Magistrate for trial and if so taking the necessary steps

		for the same by the filing of a charge-sheet under Section 173." This Court, however, has not said that if a police officer takes merely one or two of the steps indicated by it, what he has done must necessarily be regarded as investigation. Investigation, in substance, means collection of evidence relating to the commission of the offence. The Investigating Officer is, for this purpose, entitled to question persons who, in his opinion, are able to throw light on the offence which has been committed and is likewise entitled to question the suspect and is entitled to reduce the statements of persons questioned by him to writing. He is also entitled to search the place of the offence and to search other places with the object of seizing articles connected with the offence. No doubt, for this purpose he has to proceed to the spot where the offence was committed and do various other things. But the main object of investigation being to bring home the offence to the offender the essential part of the duties of an Investigating Officer in this connection is, apart from arresting the offender, to collect all material necessary for establishing the accusation against the offender. Merely making some preliminary enquiries upon receipt of information from an anonymous source or a source of doubtful reliability for checking up the correctness of the information does not amount to collection of evidence and so cannot be regarded as investigation. In the absence of any prohibition in the Code, express or implied, I am of opinion that it is open to a police officer to make preliminary enquiries before registering an offence and making a full scale investigation into it…"
2.	**Babubhai v. State of Gujarat, (2010) 12 SCC 254**	Not only fair trial but fair investigation is also part of constitutional rights guaranteed

		under Articles 20 and 21 of the constitution of India. Therefore, investigation must be fair, transparent and judicious as it is the minimum requirement of rule of law. The investigating agency cannot be permitted to conduct an investigation in a tainted and biased manner
FURTHER INVESTIGATION		
3.	**Ram Lal Narang vs. State (Delhi Administration) (1979) 2 SCC 322**	Where fresh materials come to light which would implicate persons not previously accused or absolve persons already accused or where it comes to the notice of the investigating agency that a person already accused of an offence has a good alibi, it may be the duty of the investigating agency to investigate the genuineness of the same and submit a report to the court.
4.	**Central Bureau of Investigation v. R S Pai (2002) 5 SCC 82**	**DOCUMENTS CAN BE SUBMITTED SUBSEQUENTLY** "7. From the aforesaid sub-sections, it is apparent that normally, the investigating officer is required to produce all the relevant documents at the time of submitting the charge- sheet. At the same time, as there is no specific prohibition, it cannot be held that the additional documents cannot be produced subsequently. If some mistake is committed in not producing the relevant documents at the time of submitting the report or the charge-sheet, it is always open to the investigating officer to produce the same with the permission of the court.
5.	**Hasan Bhai Valibhai Qureshi vs. State of Gujarat & Ors.,** **(2004) 5 SCC 347**	Further investigation is not altogether ruled out merely because cognizance has been taken by the court. When defective investigation comes to light during course of trial, it may be cured by further investigation, if circumstances so permitted.

6.	**Sameer Sandhir v. CBI** **2025 INSC 776**	**SECTION 173(5) IS DIRECTORY** The Hon'ble Supreme Court has upheld the decision of High Court and Trial Court allowing the CBI to produce two Compact Discs (CDs) as evidence in a corruption trial, even though they were not filed with Charge Sheet or Supplementary Charge Sheet. Held that provision of Sec. 173(5) CrPC is directory not mandatory.
ARREST		
7.	**Mihir Rajesh Shah Versus State of Maharashtra & Anr,** **2025 INSC1288**	**THE GROUND OF ARREST MUST BE COMMUNICATED IN WRITING TO THE ARRESTEE IN THE LANGUAGE HE/SHE UNDERSTANDS….** The said grounds be communicated in writing within a reasonable time and in any case at least two hours prior to production of the arrestee for remand proceedings before the magistrate. In case of noncompliance with the mandate, the arrest and subsequent remand would become illegal and entitle the person to be set free.
8.	**Arshad Neyaz Khan V. State of Jharkhand** **2025 INSC 1151**	**OFFENCES OF 'CHEATING' & 'CRIMINAL BREACH OF TRUST' CANNOT CO-EXIST ON SAME ALLEGATIONS** The Hon'ble Court held that the offence of cheating (S.420 IPC/S.318 BNS) involves criminal intention from inception; however, for criminal breach of trust (S.406 IPC/S.316 BNS), there is lawful entrustment at the beginning, which is later misappropriated. So, both these offences cannot exist simultaneously on same facts.
9.	**Delhi Race Club (1940) Ltd. v. State of U.P.** **(2024) 10 SCC 690**	**OFFENCES OF 'CHEATING' & 'CRIMINAL BREACH OF TRUST' ARE ANTITHETICAL TO EACH OTHER** There is a distinction between criminal breach of trust and cheating. For cheating,

		criminal intention is necessary at the time of making false or misleading representation i.e. since inception. In criminal breach of trust, mere proof of entrustment is sufficient. Thus, in case of criminal breach of trust, the offender is lawfully entrusted with the property, and he dishonestly misappropriates the same. Whereas, in case of cheating, the offender fraudulently or dishonestly induces a person by deceiving him to deliver a property. In such a situation, both offences cannot co-exist simultaneously.
10.	**Jit Vinayak Arolkar v. State of Goa, 2025 SCC OnLine SC 31**	**CRIMINAL COMPLAINT IN CIVIL DISPUTE** In a dispute between co-owner of disputed property/sale deed and appointed power of attorney, criminal complaint against appointed power of attorney for the offence of cheating under S. 415 of IPC, 1860 filed after a time gap of two years from date of institution of civil suits. Held, when there was a dispute over the title, setting in motion criminal proceedings two years after the date of filing of the suits amounts to nothing but abuse of the process of law- FIR quashed.
		BAIL
11.	**State of Rajasthan vs. Balchand, (1977) 4 SCC 308**	Hon'ble Supreme Court has observed that the basic rule of our criminal justice system is 'bail, not jail'.
12.	**Hitendra Vishnu Thakur vs. State of Maharashtra, (1994) 4 SCC 602**	**DEFAULT BAIL** Default bail cannot be granted automatically an accused is required to make an application if he wishes to be released on bail on account of the 'default' of the investigating/prosecuting agency and such bail shall be dealt under Chapter XXXIII of the Criminal Procedure Code.
13.	**Kartar Singh vs. State of Punjab (1994) 3 SCC 569**	**ACCUSED OF SERIOUS OFFENCES** The Hon'ble Supreme Court upheld the validity of the Terrorist and Disruptive Activities (Prevention) Act (TADA) but also

		laid down guidelines to prevent the misuse of the Act. The Court insisted on the protection of fundamental rights, even for those accused of serious offenses under TADA.
14.	**Babua Tazmul Hossain vs. State of Orissa,** **Appeal (Crl.) 593 of 2002,**	The Hon'ble Supreme Court observed that "pre-trial detention should not be reinstated as a punishment measure. The accused should also be granted the privilege of bail to better defend his case."
15.	**Gautam Navlakha Vs. NIA (2022) 13 SCC 542**	**RIGHT TO DEFAULT BAIL** Right to default bail is fundamental right subject to fulfilment of conditions in Section 167 CrPC
16.	**Dinesh Dalmia vs. C.B.I.,** **AIR 2008 SC 78**	The Hon'ble Supreme Court laid down that investigating agency is required to complete investigation within reasonable time…….If the investigation is not completed within stipulated period the same would not be detrimental to right of accused to bail. On expiry of stipulated period he would be entitled for bail, but Right to bail does not revive only because a further investigation remains pending. When a charge sheet is not filed and investigation is kept pending, the accused will have right to bail u/s 167(2). Once, a charge sheet is filed, the said right ceases. Such a right does not revive only because a further investigation remains pending within the meaning of Sub-section (8) of Section 173 of the Code of Criminal procedure.
17.	**Rasiklal V/s Kishore Khanchand Wadhwani (AIR 2009 1341)**	"As soon as it appears that the accused person is prepared to give bail, the police officer or the court before whom he offers to give bail, is bound to release him on such terms as to bail as may appear to the officer or the court to be reasonable. It would even be open to the officer or the court to discharge such person on his

		executing a bond as provided in the Section instead of taking bail from him".
18.	**Atul Tripathi Vs. State of UP Crl. Appeal No.NO.1516/2014 Dated.22-07-2014**	Hon'ble Supreme Court has discussed the scope and ambit of Section 389 ofCr.P.C and issued the following Guidelines regarding the suspension of Sentence during the pendency of Criminal Appeal. I. The appellate court, if inclined to consider the release of a convict sentenced to punishment for death or imprisonment for life or for a period of ten years or more, shall first give an opportunity to the public prosecutor to show cause in writing against such release. II. On such opportunity being given, the State is required to file its objections, if any, in writing. III. In case the public prosecutor does not file the objections in writing, the appellate court shall, in its order, specify that no objection had been filed despite the opportunity granted by the court. IV. The court shall judiciously consider all the relevant factors whether specified in the objections or not, like gravity of offence, nature of the crime, age, criminal antecedents of the convict, impact on public confidence in court, etc. before passing an order for release.
19.	**S. Kasi v. State Through The Inspector of Police Samaynallur Police Station Madurai District,2020 SCC OnLine SC 529,**	Hon'ble Supreme Court has observed that the indefeasible right to default bail under Section 167(2) is an integral part of the right to personal liberty under Article 21, and the said right to bail cannot be suspended even during a pandemic situation as is prevailing currently. It was emphasized that the right of the accused to be set at liberty takes precedence over the right of the State to carry on the investigation and submit a chargesheet.

20.	**Prabhakar Tewari vs St of U.P& Another (2020)11SCC,648,**	"The pendency of several criminal cases against an accused by itself cannot be a basis for refusal of bail."
21.	**Satender Kumar Antil v. CBI, (2022) 10 SCC 51**	Hon'ble Supreme Court of India laid down comprehensive guidelines regarding grant of bail and arrest procedures, reinforcing the principle that "bail is the rule and jail is the exception." The Court emphasized that unnecessary arrests and prolonged incarceration violate Article 21 of the Constitution. 1. Categorisation of Offences: The Court classified offences into categories (A to D) based on severity and punishment to guide courts in granting bail. 2. Mandatory Compliance with Sections 41 & 41A CrPC: Police must justify arrest and issue notice of appearance in offences punishable up to 7 years, as per Arnesh Kumar v. State of Bihar. 3. Default Bail & Charge Sheet Filing: Filing of charge sheet does not automatically justify custody if the accused cooperated during investigation. 4. Undertrial Detention: Courts must prevent prolonged incarceration of undertrial prisoners. 5. Special Acts: Even under special statutes (e.g., PMLA, NDPS), procedural safeguards must be respected unless specific statutory restrictions apply.
22.	**Arvind Kumar v. State of Rajasthan, (2022) 16 SCC 732**	6. The petitioner, Arvind Kumar, was in judicial custody in connection with FIR No. 185/2022 at Bichiwara Police Station, Dungarpur, involving offences under Sections 341, 323, 326 and 308 read with Section 34 of the IPC. His earlier bail application was dismissed, and after the

		charge-sheet was filed the present second bail plea was moved. The Court noted the prolonged trial and that the injured had been discharged from hospital. On weighing facts and circumstances and without expressing any view on merits, the Court granted bail under Section 439 of the CrPC, directing him to execute a personal bond with sureties pending trial.
23.	**Vivekanand Mishra vs State of UP and Another,** **2022 SCC OnLine SC 1903,**	It is a basic principle of criminal law, that bail is the rule and jail an exception. At the same time the non negotiable right of an individual to liberty must be juxtaposed with societal interest. Grant of Anticipatory Bail in a heinous case like this, on the basis of a CCTV footage produced by the Accused-Respondent, without any kind of certification and/or authentication, ignoring the materials on record including a dying declaration made by the deceased in hospital before the Tehsildar and statements of an eye-witness, can in no circumstances be justified.
24.	**Sumitha Pradeep Versus Arun Kumar C.K. and Another,** **2022 SCC OnLine SC 1529,**	Hon'ble supreme Court in para 16, held that "We are dealing with a matter wherein the original complainant (appellant herein) has come before this Court praying that the anticipatory bail granted by the High Court to the accused should be cancelled. To put it in other words, the complainant says that the High Court wrongly exercised its discretion while granting anticipatory bail to the accused in a very serious crime like POCSO and, therefore, the order passed by the High Court granting anticipatory bail to the accused should be quashed and set aside. In many anticipatory bail matters, we have noticed one common argument being canvassed that no custodial interrogation is required and, therefore, anticipatory bail may be granted. There appears to be a serious misconception of law that if no case

		for custodial interrogation is made out by the prosecution, then that alone would be a good ground to grant anticipatory bail. Custodial interrogation can be one of the relevant aspects to be considered along with other grounds while deciding an application seeking anticipatory bail. There may be many cases in which the custodial interrogation of the accused may not be required, but that does not mean that the prima facie case against the accused should be ignored or overlooked and he should be granted anticipatory bail. The first and foremost thing that the court hearing an anticipatory bail application should consider is the prima facie case put up against the accused. Thereafter, the nature of the offence should be looked into along with the severity of the punishment. Custodial interrogation can be one of the grounds to decline anticipatory bail. However, even if custodial interrogation is not required or necessitated, by itself, cannot be a ground to grant anticipatory bail.”
25.	**Re Policy Strategy for Grant of Bail SMW, 2023 (2) KLT 97,**	**SEVEN DIRECTIONS TO AVOID DELAY IN RELEASE OF PRISONERS AFTER GETTING BAIL** Hon’ble Court has issued following directions for speedy release of an accused detained in jail: (i)The Court which grants bail to an under trial prisoner/convict would be required to send a soft copy of the bail order by e-mail to the prisoner through the Jail Superintendent on the same day or the next day. The Jail Superintendent would be required to enter the date of grant of bail in the e-prisons software [or any other software

		which is being used by the Prison Department]. (ii) If the accused is not released within a period of 7 days from the date of grant of bail, it would be the duty of the Superintendent of Jail to inform the Secretary, DLSA who may depute para legal volunteer or jail visiting advocate to interact with the prisoner and assist the prisoner in all ways possible for his release. (III.) NIC would make attempts to create necessary fields in the e-prison software so that the date of grant of bail and date of release are entered by the Prison Department and in case the prisoner is not released within 7 days, then an automatic email can be sent to the Secretary, DLSA. (iv)The Secretary, DLSA with a view to find out the economic condition of the accused, may take help of the Probation Officers or the Para Legal Volunteers to prepare a report on the socio-economic conditions of the inmate which may be placed before the concerned Court with a request to relax the condition (s) of bail/surety. (v) In cases where the under trial or convict requests that he can furnish bail bond or sureties once released, then in an appropriate case, the Court may consider granting temporary bail for a specified period to the accused so that he can furnish bail bond or sureties. (vi) If the bail bonds are not furnished within one month from the date of grant bail, the concerned Court may suo moto take up the

		case and consider whether the conditions of bail require modification/ relaxation. (Vii) One of the reasons which delays the release of the accused/ convict is the insistence upon local surety. It is suggested that in such cases, the courts may not impose the condition of local surety.
26.	**Ritu Chhabaria Versus Union of India and Others,2023 SCC OnLine SC 502**	**FILING CHARGESHEET WITHOUT COMPLETING THE INVESTIGATION DOES NOT EXTINGUISH THE RIGHT OF AN ACCUSED FOR GRANT OF DEFAULT BAIL** Without completing the investigation of a case, a chargesheet or prosecution complaint cannot be filed by an investigating agency only to deprive an arrested accused of his right to default bail under Section 167(2) of the CrPC. Such a chargesheet, if filed by an investigating authority without first completing the investigation, would not extinguish the right to default bail under Section 167(2) CrPC.The trial court, in such cases, cannot continue to remand an arrested person beyond the maximum stipulated time without offering the arrested person default bail.
27.	**Manish Sisodia vs Directorate of Enforcement, 2024 INSC 545,**	"The bail is not to be withheld as a punishment is not to be forgotten, Bail is a rule & jail is an exception."
28.	**Parvinder Singh Khurana v. Directorate of Enforcement, 2024 SCC OnLine SC 1765 : 2024 INSC 546,**	The Para -11, an order granting a stay to the operation of the order granting bail during the pendency of the application for cancellation of bail should be passed in very rare cases. 12, An order granting bail can be stayed by the Court only in exceptional cases when a very strong prima facie case of the existence of the grounds for cancellation of bail is made out. The prima facie case must be of a

		very high standard. By way of illustration, we can point out a case where the bail is granted by a very cryptic order without recording any reasons or application of mind. One more illustration can be of a case where material is available on record to prove serious misuse of the liberty made the accused by tampering with the evidence, such as threatening the prosecution witnesses. If the High Court or Sessions Court concludes that an exceptional case is made out for the grant of stay, the Court must record brief reasons and set out the grounds for coming to such a conclusion. 13. An ex-parte stay of the order ranting bail, as a standard rule, should not be granted. The power to grant an ex-parte interim stay of an order granting bail has to be exercised in very rare and exceptional cases where the situation demands the passing of such an order. While considering the prayer for granting an ex-parte stay, the concerned Court must apply its mind and decide whether the case is very exceptional, warranting the exercise of drastic power to grant an ex-parte stay of the order granting bail. Liberty granted to an accused under the order granting bail cannot be lightly and casually interfered with by mechanically granting an ex-parte order of stay of the bail order.
29.	**Sanjeev Kumar Vs. State** **2024 SCC OnLine Del 7323**	The Hon'ble Delhi High Court analyzed the bail application in light of the Bharatiya Nagarik Suraksha Sanhita (BNSS) 2023, which governs the rights of detainees and the maximum permissible detention period for undertrials. The court considered that the accused, arrested in a serious financial fraud case, had been in detention for an extended period without trial. The provisions of BNSS, especially regarding prolonged

		pretrial detention, were central to the defense argument, which highlighted the need for a balanced approach, considering the applicant's right to a fair trial and personal liberty.
30.	**Himanshu Sharma Vs. State of MP, (2024) 4 SCC 222**	(Paras 10 & 11), the Hon'ble Supreme Court has held that the law is well settled that the considerations for grant of bail and cancellation thereof are entirely different. Bail granted to an accused can only be cancelled if the court is satisfied that after being released on bail, (i) the accused has misused the liberty granted to him; (ii) flouted the conditions of bail order; (iii) that the bail was granted in ignorance of statutory provisions restricting the powers of the Court to grant bail; (iv) or that the bail was procured by misrepresentation or fraud."
31.	**CBI v. Kapil Wadhawan, (2024) 3 SCC 734, 2024 SCC OnLine SC 66**	Para15. There cannot be any disagreement with the well-settled legal position that the right of default bail under Section 167(2)CrPC is not only a statutory right but is a right that flows from Article 21 of the Constitution of India. It is an indefeasible right, nonetheless it is enforceable only prior to the filing of the challan or the charge-sheet, and does not survive or remain enforceable on the challan being filed, if already not availed of. Once the challan has been filed, the question of grant of bail has to be considered and decided only with reference to the merits of the case under the provisions relating to grant of bail to the accused after the filing of the challan. **Para 22.** In view of the above settled legal position, there remains no shadow of doubt that the statutory requirement of the report under Section 173(2) would be complied with if the various details prescribed therein

		are included in the report. The report under Section 173 is an intimation to the court that upon investigation into the cognizable offence, the investigating officer has been able to procure sufficient evidence for the court to inquire into the offence and the necessary information is being sent to the court. The report is complete if it is accompanied with all the documents and statements of witnesses as required by Section 175(5). As settled in the aforestated case, it is not necessary that all the details of the offence must be stated. **Para 23.** The pendency of the further investigation qua the other accused or for production of some documents not available at the time of filing of charge-sheet would neither vitiate the charge-sheet, nor would it entitle the accused to claim right to get default bail on the ground that the charge-sheet was an incomplete charge-sheet or that the charge-sheet was not filed in terms of Section 173(2)CrPC.
RECORDING OF SEARCH AND SEIZURE THROUGH AUDIO-VIDEO ELECTRONIC MEANS		
32.	**Satya Narain Musadi & Ors. vs. State of Bihar (1980) 3 SCC 152**	Statutory requirement of the report under Section 173(2) would be complied with if various details prescribed therein are included in the report. The report is complete if it is accompanied with all the documents and statements of witnesses as required by Section 175(5).

PROVISIONS UNDER BNSS, 2023		
33.		➢ RECORDING OF SEARCH AND SEIZURE THROUGH AUDIO-VIDEO ELECTRONIC MEANS (S. 105 BNSS) ➢ SEARCH BY POLICE OFFICER (S. 185 BNSS)
34.		**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 (C.VII) 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 the District Magistrate, Sub-divisional Magistrate or Judicial Magistrate of the first class.
35.		**SECTION 185 of BNSS (S. 165 CRPC)** **SEARCH BY POLICE OFFICER** **(1) Whenever an officer in charge of a police station or a police officer** ➢ Making an investigation has reasonable grounds for believing that ➢ Anything necessary for the purposes of an investigation into any offence ➢ Which he is authorised to investigate may be found in any place ➢ Within the limits of the police station of which he is in charge, or ➢ To which he is attached, and that such thing cannot in his opinion be otherwise obtained without undue delay, ➢ Such officer may, after recording in writing the grounds of his belief in the case-diary and

		➢ specifying in such writing, so far as possible, the thing for which search is to be made, search, or cause search to be made, for such thing in any place within the limits of such station. (2) 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) If he is unable to conduct the search in person, and ➢ There is no other person competent to make the search present at the time, ➢ He may, after recording in writing his reasons for so doing, ➢ Require any officer subordinate to him to make the search, and ➢ He shall deliver to such subordinate officer an order in writing, ➢ Specifying the place to be searched, and ➢ So far as possible, the thing for which search is to be made; and ➢ Such subordinate officer may thereupon search for such thing in such place. (4) The provisions of this Sanhita as to search-warrants and the general provisions as to searches contained in section 103 shall, so far as may be, apply to a search made under this section. (5) Copies of any record made under sub-section (1) or sub-section (3) shall forthwith, but not later than forty-eight hours, be sent to the nearest Magistrate empowered to take cognizance of the offence, and the owner or occupier of the place searched shall, on application, be furnished, free of cost, with a copy of the same by the Magistrate.
FUTURE OF EVIDENCE GENERATION		
36.		National Informatics Centre (NIC): Applications

		➢ E-Sakshya-To enable electronic videography/photography of crime scenes. ➢ NyayShruti- To enable conduct of judicial hearings. ➢ e-Summon- To deliver court summons electronically. NyayaSetu- Dashboard that connects authorities like police, medical, forensic, prosecution, and prison to provide the real-time information on investigations.
GENERAL PROCEDURE TO CONDUCT SEARCH & SEIZURE (As Per SOP)		
37.		**VIDEOGRAPHY** ➢ Begin recording before entering the premises. ➢ 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. ➢ The video-recording so made shall be part of the case diary. ➢ 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.
38.		**POST VIDEOGRAPHY** ➢ Review the recording for accuracy and completeness. ➢ Securely store and backup the recording. ➢ Label the recording with date, time, location, case details, and a brief description of the content.

<table>
<tr><th colspan="3">PROCEDURE OF STORAGE &TRANSPORTATION</th></tr>
<tr><td>39.</td><td></td><td>The police officer will, without delay, but not later than 48 hours, send to the Magistrate copy of the list of seized items with the signature of the witnesses and video-recording of the search and seizure process, as per procedure below-
i. On completion of the search and seizure operation, the police officer will bring the audio-video electronic device which was used for recording to the Police Station.
ii. At the Police Station, the AV recording will be transferred to the local designated desktop - either directly through device insertion or via Cable or Bluetooth. Mention of this will be made in chain of custody form & Hashing will be done.
iii. 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_.....ddmmyy_....SNo......
iv. 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.
v. The AV recording will be scanned for any virus before any further processing.
vi. The AV recording will then be deleted from the police officer's smartphone or audio-video recorder, making space for more recordings to be made in the future.
vii. The following day, the designated data manager of the police station will transfer all such recordings of the last 24 hours on a portable storage devise and proceed to download all the recordings on the storage device of the Magistrate.</td></tr>
<tr><th colspan="3">TASKS DURING STORAGE & TRANSPORTATION</th></tr>
<tr><td>40.</td><td></td><td>Prepare Master Negative-</td></tr>
</table>

		The evidence specialist, or the designated officer, will copy, without opening, the digital images/ Video onto a Hard Disk or Pen drive or Storage Devices which will become the "Master Negative." **Prepare Negative Duplicate or Mirror Image (Working Record)-** The files on the Master Negative Pen drive or Storage Devices should be copied, without opening, onto another Pen drive or storage devices which becomes the working record, the "negative duplicate or mirror image." **Prepare Separate Record for each Case/Investigation** A separate Hard Disk or Pen Drive or Storage Device should be created from the negative duplicate Pen drive or storage devices for each criminal case or investigation. **Hashing-** The hashing should be done at the stage, while transferring data from mobile/audio-video recorder to dedicated computer/hard disk or storage device, using various tools and softwares. **Prepare 'Chain of Custody' Forms-** Transfers should be depicted in chain of custody forms with responder & evidence expert signing duly. **Custody of Appropriate Department or Officer-** Once the master negative disk or Pen drive or storage device has been created, it shall not be removed from the custody of the appropriate department or officer.
CHAIN OF CUSTODY FORM		
41.		**Case Details** FIR No. Police Station

		Name of I.O. Date of Seizure Time Place **Device Details** Item No. Device Type Make Model Device Sr. No. Description Remarks **Chain of Custody Documentation** Item No. Received From Received By Reason Date/Time Sign. of Receiver Remarks
CERTIFICATION of AUDIO- VIDEO CONTENT		
42.		➢ Each audio-video recording as part of procedural compliance and investigative compliance and each seizure of relevant digital evidence requires certification, doubly- ➢ Section 63(4)(c) - Part -A ➢ Owner/operator/handler or manager or person in-charge of communication /computer device in contention. Section 63(4)(c) - Part -B ➢ Expert.
43.		National Informatics Centre (NIC): Applications ➢ E-Sakshya-To enable electronic videography/photography of crime scenes. ➢ NyayShruti- To enable conduct of judicial hearings. ➢ e-Summon- To deliver court summons electronically.

		➢ NyayaSetu- Dashboard that connects authorities like police, medical, forensic, prosecution, and prison to provide the real-time information on investigations.
DEFECTIVE SEARCH & SEIZURE		
44.	**State of M.P. vs. Paltan Mallah (2005) 3 SCC 169**	"...the evidence obtained under illegal search could still be admitted in evidence provided there is no express statutory violation or violation of the constitutional provisions. For example, if certain specific enactments are made and the search or seizure is to be effected in accordance with the provisions of such enactment, the authorities shall comply with such provisions. The general provisions given in the Criminal Procedure Code are to be treated as guidelines and if at all there is any minor violation, still the court can accept the evidence and the courts have got discretionary power to either accept it or reject it."
45.	**Radha Krishan vs. State of U.P. AIR 1963 SC 822**	"So far as the alleged illegality of the search is concerned, it is sufficient to say that even assuming that the search was illegal and the seizure of the articles is not vitiated. It may be that where the provisions of Sections 103 and 165 of the Code of Criminal Procedure are contravened the search could be resisted by the person whose premises are being searched. It may also be that because of the illegality of the search the Court may be inclined to examine carefully the evidence regarding the seizure. But beyond these two consequences, no further consequence ensues."
46.	**Pooran Mal vs. Director of Inspection (1974) 1 SCC 354**	"So far as India is concerned its law of evidence is modeled on the rules of evidence which prevailed in English Law, and Courts in India and in England have consistently refused to exclude relevant evidence merely on the ground that it is obtained by illegal

		search or seizure . It would thus be seen that in India, as in England, where the test of admissibility of evidence lies in relevancy, unless there is an express or necessarily implied prohibition in the Constitution or other law, evidence obtained as a result of illegal search or seizure is not liable to shut out."
47.	**Maharashtra v. Tapas D. Neogy, (1999) 7 SCC 685.**	**POWERS OF POLICE OFFICER TO SEIZE "ANY PROPERTY** A police officer under this section has the power to seize any property which may be found under circumstances creating suspicion of the commission of any offence. The legislature having used the expression "any property" and "any offence" have made the applicability of the provisions wide enough to cover offences created under any Act,
48.	**Dinesh Dalmia vs. CBI** **(2007) 8 SCC 770**	Even if all the documents are not filed, by reason thereof the submission of the chargesheet itself would not be vitiated in law.
49.	**Teesta Atul Setalvad v. State of Gujarat, (2018) 2 SCC 372**	property" includes any bank account creating suspicion about commission of an offence. Bank account need not be only of accused but can be any account creating suspicion about commission of offence,
50.	**Nevada Properties (P) Ltd. v. State of Maharashtra,** **(2019) 20 SCC 119.**	Power of police officer to seize "any property" does not include power to attach, seize and seal immovable property,
51.	**Firoz Hira Manik Vs State of U.P(2024)**	The Hon'ble Supreme Court dismissed the evidence presented without any recording and re-emphasized on the mandatory nature of the electronic recording
COGNIZATION ON COMPLAINT & PROCEDURE		

TO BE ADPOTED		
52.		(1) A Magistrate having jurisdiction while taking cognizance of an offence on complaint shall examine upon oath the complainant and the witnesses present, if any, and the substance of such examination shall be reduced to writing and shall be signed by the complainant and the witnesses, and also by the Magistrate: Provided that no cognizance of an offence shall be taken by the Magistrate without giving the accused an opportunity of being heard: Provided further that when the complaint is made in writing, the Magistrate need not examine the complainant and the witnesses— (a) if a public servant acting or purporting to act in the discharge of his official duties or a Court has made the complaint; or (b) if the Magistrate makes over the case for inquiry or trial to another Magistrate under section 212: Provided also that if the Magistrate makes over the case to another Magistrate under section 212 after examining the complainant and the witnesses, the latter Magistrate need not re-examine them (2) A Magistrate shall not take cognizance on a complaint against a public servant for any offence alleged to have been committed in course of the discharge of his official functions or duties unless— (a) such public servant is given an opportunity to make assertions as to the situation that led to the incident so alleged; and (b) a report containing facts and circumstances of the incident from the officer superior to such public servant is received.”
53.	**Sri Basanagouda R Patil (Yatnal) vs Sri Shivananda S Patil**	“10. Therefore, the procedural drill would be this way: A complaint is presented before the Magistrate under Section 223 of the BNSS;

	on 27 September, 2024 Criminal Petition No.7526 OF 2024	on presentation of the complaint, it would be the duty of the Magistrate / concerned Court to examine the complainant on oath, which would be his sworn statement and examine the witnesses present if any, and the substance of such examination should be reduced into writing. The question of taking of cognizance would not arise at this juncture. The magistrate has to, in terms of the proviso, issue a notice to the accused who is given an opportunity of being heard. Therefore, notice shall be issued to the accused at that stage and after hearing the accused, take cognizance and regulate its procedure thereafter. 11. The proviso indicates that an accused should have an opportunity of being heard. Opportunity of being heard would not mean an empty formality. Therefore, the notice that is sent to the accused in terms of proviso to sub-section (1) of Section 223 of the BNSS shall append to it the complaint; the sworn statement; statement of witnesses if any, for the accused to appear and submit his case before taking of cognizance. In the considered view of this Court, it is the clear purport of Section 223 of BNSS 2023."
54.	**SUBY ANTONY v. 1 R1(DELETED), CRL.MC NO. 508 OF 2025**	"7. Indeed, a radical change in procedure is brought about by the proviso to Section 223(1) of BNSS. Pertinently, in spite of the proviso to Section 223(1) making it mandatory to provide opportunity of hearing to the accused before taking cognizance, Section 226 does not reckon the accused's objection at the stage of taking cognizance as a relevant factor for dismissing the complaint. Being guided by the precedents on Sections 200 and 202 of the Code and the plain language of the proviso to Section 223(1) of the BNSS, this Court is of the opinion that, after the complaint is filed, the Magistrate should first examine the complainant and witnesses on oath and thereafter, if the Magistrate proceeds to take cognizance of the offence/s, opportunity of hearing should be afforded to the accused."

55.	**Sanjabij Tari Vs. Kishore S. Borcar & Another. 2025 INSC 1158**	No need for pre cognizance summons to accused in 138 N.I. Act. The Hon'ble Supreme Court observed that an accused need not be heard at the pre cognizance stage of complaints filed for dishonour of cheque as per Section 138 of N.I. Act.
56.	**Kushal Kumar Agarwal v. Enforcement Directorate, 2025 SCC OnLine SC 1221**	The Hon'ble Supreme Court held that before a cognizance is taken of the offence of money laundering under the PMLA, the accused must be given an opportunity to be heard, a right created by the proviso to Section 223(1) of the BNSS.(Para 12).
57.	**Parvinder Singh v. Enforcement Directorate, 2026 SCC OnLine SC 903**	**Para-38.** "Based on the above discussion, the views expressed by the High Court are, therefore, liable to be set aside. We do find that the allegations against the appellant are quite serious. However, non-compliance with the first proviso to Section 223(1) of the BNSS vitiates the very order taking cognizance, and the same cannot be sustained in the eyes of the law. In fact, the appellant has, at the earliest point in time, filed the application for recall of the order taking cognizance by placing reliance upon the said proviso. Had the Special Court allowed it, the trial would have proceeded further. Suffice it to state that the appellant cannot be faulted for any delay that has occasioned."

CYBER LAW & CYBER CRIME

Introduction

Technology advancement not only broaden scientific horizon but also give rise to challenges for the legal system. Information Technology includes Computers, Internet and Cyber space. The present challenges for law is to tackle information technology. These challenges are not confined to any single traditional legal category but in almost all categories of law. To tackle with this new definition and understanding of the accepted norms of criminal conduct and punishment is required. The criminal activities in relation to the cyber space can be dealt with by framing legal rules, strengthening the administrative frame, work and convicting the accused by way of quick and efficient justice delivery system. The judiciary throughout the world have been dealing with these problems.

Meaning of Cyber Law

As internet grows, numerous legal issues arise. One of the most important issues concerning cyberspace today is that of cybercrime. Cybercrimes refer to all the activities done with criminal intent in cyberspace. Cybercrimes mainly include transmission of the pornographic and obscene matters, online harassment, hacking and cyber terrorism. Computer crime can also involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief.

There is no exhaustive definition of the term Cyber Law. The word Cyber Law relates to machines. However, simply put, Cyber Law is a term which refers to all the legal and regulatory aspects of internet and the World Wide Web. Anything concerned with or related to, or emanating from, any legal aspects or issues concerning any activity of netizens and others, in Cyberspace comes within the ambit of Cyber Law.

Cyber Law is a term first coined by Jonathan Rosenoer as the title for a service aimed at explaining legal issues to computer user. He derived it from the term, “Cybernetics”.

In Concise English Dictionary Cyber Law is defined as CYBERNETICS, the science of communication and automatic control system in both machines and living things. Today there is convergence of technical, function and regulatory aspect of communication. Cyber Law is the law relating to communications and automatic control systems. It is the law governing cyberspace.

Cyber Law is a generic term, and it governs a boundless, timeless, space less, medium which has emanated to encompass the future business, known as Cyber medium of Cyber space. The term CYBERSPACE was first coined by the science fiction author William Gibson in his novel NUROMANCER in 1982 to describe the environment within which computer hackers operate. Cyberspace is the wide term and includes computers, networks, software, data storage devices, the internet, websites, emails and even electronic devices.

History of Cyber Crime

“Cyber Crime” is any illegal activity that uses a computer, network or electronic communications device to commit a crime.

Cybercrime cannot be described as a single definition, it is best considered as a collection of acts or conducts. These acts are based on the material offence object that affects the computer data or systems. These are the illegal acts where a digital device or information system is a tool or a target or it can be the combination of both. The cybercrime is also known as electronic crimes, computer-related crimes, e-crime, high-technology crime, information age crime etc.

In simple term “Cyber Crimes” mean the offences or crimes that takes place over electronic communications or information systems. These types of crimes are basically the illegal activities in which a computer and a network are involved. Due of the development of the internet, the volumes of the cybercrime activities are also increasing because for committing a crime there is no need for the physical present of the criminal.

The unusual characteristic of cybercrime is that the victim and the offender may never come into direct contact. Cyber criminals often opt to operate from countries with nonexistent or weak cybercrime laws in order to reduce the chances of detection and prosecution.

The first Cyber Crime was recorded within the year 1820. The removal type of computer has been in Japan, China and India since 3500 C.C, but Charles Babbage’s analytical engine is considered as the time of present day computers. In the year 1820, in France a textile manufacturer named Joseph-Marie Jacquard created the loom. This device allowed a series of steps that was continual within the weaving of special fabrics or materials. This resulted in an exceeding concern among the Jacquard’s workers that their livelihoods as well as their traditional employment were being threatened, and prefer to sabotage so as to discourage Jacquard so that the new tech. The unusual characteristic of cybercrime is that the victim and the offender may never come into direct contact. Cybercriminals often opt to operate from countries with nonexistent or weak cybercrime laws in order to reduce the chances of detection and prosecution. Ology cannot be utilized in the future.

Evolution of Cyber Crime

The cyber crime is evolved from Morris Worm to the ransom ware. Many countries including India are working to stop such crimes or attacks, but these attacks are continuously changing and effecting out nation.

Year – 1997

Types of Attacks –

Cyber crimes and viruses initiated, that includes Morris Code worm and other.

Year – 2004

Types of Attacks –

Malicious code, Torjan, Advanced worm etc.

Year – 2007

Types of Attacks –

Identifying thief, Phishing etc.

Year – 2010

Types of Attacks –

DNS Attack, Rise of Botnets, SQL attacks etc.

Year – 2013

Types of Attacks –

Social Engineering, DOS Attack, BotNets, Malicious Emails, Ransom ware attack etc.

Year – 2018 etc

Types of Attacks –

Banking Malware, Keylogger, Bitcoin wallet, Phone hijacking, Cyber warfare,

Year – 2024

Types of Attacks –

Android hack, Digital arrest, screen shot fraud &

Year – 2025

Types of Attacks –

Call merging Scam etc.

The Information Technology Act, 2000 has discussed the issues of cyber crimes in two broad groups. One in Chapter IX which deals with penalties and adjudications under sections 43 to 47 and another is Chapter XI which deals with offences under sections 65 to 75. A part from other crimes. The Information Technology Act, 2000 deals with the following cyber crimes :

a. Tempering with computer source documents,

b. Hacking

c. Publishing of information which is in electronic form.

Cyber crimes other than those mentioned under the Information Technology Act

(i).	Cyber Stalking,
(ii).	Data Diddling,
(iii).	Cyber Squatting,
(iv).	Financial Crimes,
(v).	Cyber Defamation,
(vi).	Internet Time Theft
(vii).	Torjan Attack,
(viii).	Salami Attack,
(ix).	Web Jacking,
(x).	Virus/Wrom Attack,
(xi).	E-mail Bombing,
(xii).	E-mail Spoofing,
(xiii).	Cyber Terrorism,
(xiv).	Call merging Scam.

A. TEMPERING WITH COMPUTER SOURCE DOCUMENTS :

Chapter XI of the Information Technology Act, 2000 in a magnificent way tries to cover all most all aspects of cyber crime. Section 65 of the Act provides that whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years or with fine which may be extended up to two lakh rupees, or with both. For the purposes of this section computer source code means the listing of programmes, computer commands, design and layout and programme analysis of computer source in any form.

B. HACKING:

Hacking has become associated with the act of obtaining unauthorized access to programmes or data held on computer system. Section 66 of the Information Technology Act, 2000 says that whoever with intent to cause of knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack. Generally there are three types of hackers :-

(i) the amateur group who are the latest technical proficient and confined their activities to prove their capability of penetrating system;

(ii) the browser group has moderate technical ability and gained unauthorized access to other person's files and

(iii) the cracker group who has the most technical ability and their activity ranges from copying files to damaging programmes and system.

C. Publishing of information which is obscene in electronic form :

Section 67 of the Information Technology Act, 2000 provides that whoever publishes or transmits or causes to be published in electronic form, any material which is lascivious or appeals to the prurient interest or its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second and subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

(i) Cyber Stalking:

Cyber Stalking involves following a person's movements across the internet by posting messages in the nature of threatening on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

(ii) Data Diddling:

This kind of an attack involves altering the raw data just before computer process it and then changing it back after the processing is completed.

(iii) Cyber Squatting:

Cyber squatting is the practice, by which a person, or legal entity books up the trade mark, business name, or service mark of another entity as his own domain name. It is for the purpose of holding on to it and thereafter selling the same domain name to the other person for valuable premium and consideration. Cyber squatters book domain names of important brands in the hope of earning quick millions.

(iv) Financial Crimes:

A variety of services are offered by the businesses to the consumers through internet. Internet has been misused by the dishonest traders for pertaining fraud and a new species of white-collar crime has come into existence. Internet frauds represent frauds committed by people using any of the services available on the internet. The fraud schemes include all the traditional frauds and some ingenious new ones. These include online auction frauds, online retail sales frauds, online investment frauds, business frauds, payment card frauds and others.

(v) Cyber Defamation:

Cyber defamation can be defined as any act, deed, word, gesture etc. in cyberspace, designed to harm a person's reputation on the internet or even off-line. Just as everyone in the real world has a right to an inviolate reputation, so is the case in cyber space. This type of crime is similar to cyber-venting, where instead of creating a site, email is being used to defame people.

(vi) Internet Time Theft:

This connotes the usage by an unauthorized person of the internet hours paid for by another person.

(vii) Torjan Attack:

Torjan is an unauthorized programme which functions from inside what seems to be an authorized programme, thereby concealing what it is actually doing.

(viii) Salami Attack:

This attack is used for commission of financial crimes.

The key here is to make alteration so insignificantly that in a single case it would go completely unnoticed:

(ix) Web Jacking:

This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He even mutilate or change the information on the site. This may be done for the political objectives or for money.

(x) Virus/ Worm Attack:

Virus is a programme that attaches itself to a computer on a file and then circulates itself to other files and to other computers on a network. They usually affect the data on computer, either by altering or deleting it. Worms do not need the host to attached themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

(xi) E-mail Bombing:

Email bombing refers to sending a large amount of emails to the victim resulting in the victim's email account or mail server crashing.

(xii) E-mail spoofing:

A spoofed email may be said to be one which misrepresents its origin. It shows it's origin to be different from which actually it originates. Spoofing is the act of electronically disguising one computer as another for gaining access to a restricted system

(xiii) Cyber Terrorism:

Cyber terrorism can be defined to be the premeditated use of disruptive activities or threat in cyberspace with intention to further social ideological, religious, political or similar objectives. A cyber crime is a domestic issue but cyber terrorism is a global concern.

(xiv) Call merging Scam:

Call merger fraud' is a type of phone scam where a frauster tricks a victim into merging an incoming call with their own, essentially allowing the scammer to listen in on a sensitive call, often containing personal information like bank verification Code (OTP), enabling them to make unauthorized financial transactions on the victim’s.

IRC Crime (Internet Relay Chat):

IRC servers allow the people around the world to come together under a single platform which is sometime called as rooms and they chat to each other.

- Cyber Criminals basically uses it for meeting.
- Hacker uses it for discussing their tech-niques.
- Paedophiles use it to allure small children.

A few reasons behind IRC Crime

- Chat to win ones confidence and later starts to harass sexually, and then blackmail people for ransom, and if the victim denied paying the amount, criminal starts threatening to upload victim's nude photographs or video on the internet.
- A few are paedophiles, they harass children for their own benefits.
- A few uses IRC by offering fake jobs and sometime fake lottery and earns money.

Safety in cyberspace

- ❖ Few points, one should keep in mind while surfing the internet:

- ❖ If possible always use a strong password and enable 2 steps or Two-step authentication in the webmail. It is very important in order to make your webmail or your social media account secured.

Standard for strong password

- ❖ Password should be of minimum eight characters.
- ❖ One or more than one of lower case letter, upper case letter, number, and symbol should be included.
- ❖ Replace the alike character. Example- instead of O we can use 0, instead of lower case 1 we can use I etc.
- ❖ Example of strong password: HelL0 (%there %);

Thing need to avoid while setting the

- ❖ Never use a simple password that can easily be decrypt, Example password
- ❖ Personal information should never set as a password.
- ❖ Repeating characters should be avoided.
- ❖ **Example-**aaaacc
- ❖ Using of same password in multiple sites should be avoided.

What is 2 step or Two-step authentication?

- ❖ This is an additional layer of security that requires your user name and the password also a verification code that is sent via SMS to the registered phone number. A hacker may crack your password but without the temporary and unique verification code should not be able to access your account.
- ❖ Never share your password to anyone.
- ❖ Never send or share any personal information like bank account number, ATM pin, password etc over an unencrypted connection including unencrypted mail. Websites that doesn't have the lock icon and https on the address bar of the browser are the unencrypted site. The “s” stands for secure and it indicates that the website is secure.

- Don't sign to any social networking site until and unless one is not old enough.
- Don't forget to update the operating system.
- Firewalls, anti- virus and anti-spyware software should be installed in ones PC and should be regularly updated.
- Visiting to un-trusted website or following a link send by an unknown or by an un-trusted site should be avoided.
- Don't respond to spam.
- Make sure while storing sensitive data in the cloud is encrypted.
- Try to avoid pop-ups: Pop-ups sometimes comes with malicious software. When we accept or follow the pop ups a download is performed in the background that downloaded file contains the malware or malicious software. This is called drive-by download. Ignore the pop-ups that offer site survey on ecommerce sites or similar things as they may contain the malicious code.

The Information Technology Act of India, 2000

According to Wikipedia "The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an act of the Indian Parliament (no 21 of 2000); it was notified on 17th October 2000. It is the most important law in India that deals with the digital crimes or cyber crimes and electronic commerce. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United

Nations by a resolution dated 30 January 1997".

Some key points of the Information Technology (IT) Act 2000 are as under

- E-mail is now considered as a valid and legal form of communication.
- Digital signatures are given legal validity within the Act.
- Act has given birth to new business to companies to issue digital certificates by becoming the Certifying Authorities.
- This Act allows the government to issue notices on internet through egovernance.
- The communication between the companies or between the company and the government can be done through internet.
- Addressing the issue of security is the most important feature of this Act. It introduced the construct of digital signatures that verifies the identity of an individual on internet.
- In case of any harm or loss done to the company by criminals, the Act provides a remedy in the form of money to the company.

Few important provision of IT Act

65. Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation:- For the purposes of this section, - computer source code means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Punishment

Any person who involves in such crimes could be sentenced upto 3 years imprisonment or with a fine of Rs.2 lakhs or with both.

Section 66- Computer related offences

If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Section 66A-Punishment for sending offensive messages through communication service, etc

Any person who sends, by means of a computer resource or a communication device,:-

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;

(c) any electronic mail or electronic mail message for the purpose ofcausing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Punishment

Any individual found to commit such crimes under this section could be sentenced upto 3years of imprisonment along with a fine.

Section 66B: Punishment for dishonestly receiving stolen or communication device

Whoever computer resource dishonestly receive or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Punishment

Any person who involves in such crimes could be sentenced either description for a term that may extend upto 3 years of imprisonment or with a fine of rupee 1 lakh or both.

Section 66C: Punishment for identity theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Punishment

Any person who involve in such crimes could be sentenced either with a description for a term which may extend upto 3 years of imprisonment along with a fine that mayextendupto rupee 1 lakh.

Section 66D

Punishment for cheating by personation by using computer resource. Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E: Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Section 66F- Punishment for cyber terrorism- (1) Whoever

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by:-

(i) denying or cause the denial of access to any person authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information. data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Punishment

Whoever conspires or commits such cyberc rime or cyber terrorism shall be sentenced to life time imprisonment.

Section 67- Punishment for publishing or transmitting obscene material in electronic form

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Section 67A- Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form

Whoever:-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form:-

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bona fide heritage or religious purposes.

Section 67C: Preservation and retention of information by intermediaries

(1) Intermediary shall preserve and retain such Information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.

Punishment

Whoever commits such crimes shall be sentenced for a period that may extend upto 3 years of imprisonment and also liable to fine.

Section 69: Power to issue directions for interception or monitoring or decryption of any information through any computer resource

(1) Where the Central Government or a State Government or any of its officers specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) the subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to :-

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, monitor, or decrypt the information, as the case may be; or(c) provide information stored in computer resource.

Other relevant offences under IT Act &BNS

Sec. under IT Act, 2000	Offences
Section 43	Penalty and compensation for damage to computer, computer system, etc.
Section 69 A	Power to issue directions for blocking for public access of any information through any computer resource.
Section 69 B	Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.
Section 70	Protected system
Section 71	Penalty for misrepresentation.
Section 72	Penalty for Breach of confidentiality and privacy
Section 73	Penalty for publishing electronic signature Certificate false in certain particulars.
Section 74	Publication for fraudulent purpose.
Section 75	Act to apply for offence or contravention committed outside India.
Section 77	Compensation, penalties or confiscation not to interfere with other punishment.
Section 77 A	Compounding of Offences.
Section 85	Offences by Companies
Section 503 IPC/ 351 BNS	Sending threatening messages by e-mail.
Section 499 IPC / 356 BNS	Sending defamatory messages by e-mail.
Section 420 IPC/ 318 BNS	Bogus websites, Cyber Frauds.
Section 463 IPC/ 336 BNS	E-mail Spoofing
Section 383 IPC/ 308 BNS	Web Jacking
Section 500 IPC /356 BNS	E-mail Abuse
Section 507 IPC/351 (4) BNS	Criminal intimidation by anonymous communications.
NDPS Act	Online sale of Drugs
Arm Act	Online sale of Arms

Important provisions of BSA Section 2(d) BSA defines document as:

"Document" means any matter expressed or described or otherwise recorded upon any substance by means of letters, figures or marks or any other means or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter and includes electronic and digital records.

Illustrations (i) A

writing is a document.

(i) Words printed, lithographed or photographed are documents.

(ii) A map or plan is a document.

(iii) An inscription on a metal plate or stone is a document.

(iv) A caricature is a document.

(v) An electronic record on emails, server logs, documents on computers, laptop or smartphone, messages, websites, locational evidence and voice mail messages stored on digital devices are documents;

S.32. Relevancy of statements as to any law contained in law books including electronic or digital form.—

When the Court has to form an opinion as to a law of any country, any statement of such law contained in a book purporting to be printed or published including in electronic or digital form under the authority of the Government of such country and to contain any such law, and any report of a ruling of the Courts of such country contained in a book including in electronic or digital form purporting to be a report of such rulings, is relevant.

How much of a statement is to be proved

S.33. What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers—

When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made.

S. 39.(2) When in a proceeding, the court has to form an opinion on anymatter 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 79-A of the Information Technology Act, 2000 (21 of 2000), is a relevant fact.

S.57. Primary Evidence

Primary evidence means the document itself produced for the inspection of the Court.

Explanation 4.—

Where an electronic or digital record is created or stored, and such storage occurs simultaneously or sequentially in multiple files, each such file is primary evidence.

Explanation 5.—

Where an electronic or digital record is produced from proper custody, such electronic and digital record is primary evidence unless it is disputed.

Explanation 6.—

Where a video recording is simultaneously stored in electronic form and transmitted or broadcast or transferred to another, each of the stored recordings is primary evidence.

Explanation 7.—

Where an electronic or digital record is stored in multiple storage spaces in a computer resource, each such automated storage, including temporary files, is primary evidence.

S.61. Electronic or digital record

Nothing in this Adhiniyam shall apply to deny the admissibility of an electronic or digital record in the evidence on the ground that it is an electronic or digital record and such record shall, subject to Section 63, have the same legal effect, validity and enforceability as other document.

S.63. Admissibility of electronic records.

(1) Notwithstanding anything contained in this Adhiniyam, any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media or semiconductor memory which is produced by a computer or any communication device or otherwise stored, recorded or copied in any electronic form (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely.—

(a) the computer output containing the information was produced by the computer or communication device during the period over which the computer or communication device was used regularly to create, store or process information for the purposes of any activity regularly carried on over that period by the person having lawful control over the use of the computer or communication device;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer or communication device in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer or communication device was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer or communication device in the ordinary course of the said activities.

(3) Where over any period, the function of creating, storing or processing information for the purposes of any activity regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by means of one or more computers or communication device, whether—

(a) in standalone mode; or

(b) on a computer system; or

(c) on a computer network; or

(d) on a computer resource enabling information creation or providing information processing and storage; or

(e) through an intermediary, all the computers or communication devices used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer or communication device; and references in this section to a computer or communication device shall be construed accordingly.

(4) 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.

(5) For the purposes of this section,—

(a) information shall be taken to be supplied to a computer or communication device if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) a computer output shall be taken to have been produced by a computer or communication device whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment or by other electronic means as referred to in clauses (a) to (e) of sub-section (3).

Standard of proof, authenticity and admissibility. Safeguards provided under Section 65-B.

Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 : (2014) 4 KLT 104,

Safeguards provided under Section 65-B are to ensure the source and authenticity of electronic records. As electronic records are more susceptible to tampering, alteration, transposition, excision, etc., without such safeguards, whole trial based on proof of electronic records can lead to travesty of justice,

Objections regarding admissibility of documents

Sonu v. State of Haryana, (2017) 8 SCC 570.

Objections regarding admissibility of documents which are per se inadmissible can be taken even at appellate stage. Admissibility of a document which is inherently inadmissible is an issue which can be taken up at appellate stage because it is a fundamental issue. However, mode or method of proof is procedural and objections, if not taken at trial, cannot be permitted at appellate stage. If objections to mode of proof are permitted to be taken at appellate stage by a party, the other side does not have an opportunity of rectifying deficiencies, Who can issue certificate.

Arjun PanditraoKhotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1,

The person who gives the certificate can be anyone out of several persons who occupy a "responsible official position" in relation to the operation of the relevant device, as also the person who may otherwise be in the "management of relevant activities" spoken of in Section 65-B(4)b [BSA, 2023 Section 63(4)b],

S.65. Proof of signature and handwriting of person alleged to have signed or written document produced—

If a document is alleged to be signed or to have been written wholly or in part by any person, the signature or the handwriting of so much of the document as is alleged to be in that person's handwriting must be proved to be in his handwriting.

S.66. Proof as to electronic signature

Except in the case of a secure electronic signature, if the electronic signature of any subscriber is alleged to have been affixed to an electronic record, the fact that such electronic signature is the electronic signature of the subscriber must be proved.

S.73. Proof as to verification of digital signature

In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct—

(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.

S.81. Presumption as to Gazettes in electronic or digital record

The Court shall presume the genuineness of every electronic or digital record purporting to be the Official Gazette, or purporting to be electronic or digital record directed by any law to be kept by any person, if such electronic or digital record is kept substantially in the form required by law and is produced from proper custody.

S,85. Presumption as to electronic agreements

The Court shall presume that every electronic record purporting to be an agreement containing the electronic or digital signature of the parties was so concluded by affixing the electronic or digital signature of the parties.

S.86. Presumption as to electronic records and electronic signatures

(1) In any proceeding involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceeding, involving secure electronic signature, the Court shall presume unless the contrary is proved that—

(a) the secure electronic signature is affixed by subscriber with the intention of signing or approving the electronic record;

(b) except in the case of a secure electronic record or a secure electronic signature, nothing in this section shall create any presumption, relating to authenticity and integrity of the electronic record or any electronic signature.

S.87. Presumption as to Electronic Signature Certificates

The Court shall presume, unless contrary is proved, that the information listed in an Electronic Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.

S.90. Presumption as to electronic messages

The Court may presume that an electronic message, forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

S.93. Presumption as to electronic records five years old

Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the electronic signature which purports to be the electronic signature of any particular person was so affixed by him or any person authorised by him in this behalf.

Explantion.—The explanation to Section 81 shall also apply to this section.

Relevant provision of BNSS Related to use of electronic

S.54. Identification of person arrested

Where a person is arrested on a charge of committing an offence and his identification by any other person or persons is considered necessary for the purpose of investigation of such offence, the Court, having jurisdiction may, on the request of the officer in charge of a police station, direct the person so arrested to subject himself to identification by any person or persons in such manner as the Court may deem fit:

Provided that if the person identifying the person arrested is mentally or physically disabled, such process of identification shall take place under the supervision of a Magistrate who shall take appropriate steps to ensure that such person identifies the person arrested using methods that person is comfortable with and the identification process shall be recorded by any audio-video electronic means.

S.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 the District Magistrate, Sub-divisional Magistrate or Judicial Magistrate of the first class.

Various Judgments of Hon'ble Supreme Court of India and High Courts

S NO	TITLE, CITATION
1	Syed Asifuddin v. State of Andhra Pradesh, 2005 SCC OnLine AP 1100
2	B.N. Firos v. State of Kerala, 2006 SCC OnLine Ker 159.
3	State of Punjab v. Amritsar Beverages Ltd., (2006) 7 SCC 607.
4	Avnish Bajaj v. State, 2008 SCC OnLine Del 688
5	Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473
6	RiniJohar v. State of M.P., (2016) 11 SCC 703
7	Sonu v. State of Haryana, (2017) 8 SCC 570

8	ShafhiMohd. v. State of H.P., (2018) 2 SCC 801
9	Arjun PanditraoKhotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1
10	Google India (P) Ltd. v. Visaka Industries, (2020) 4 SCC 162
11	Internet & Mobile Assn. of India v. RBI, (2020) 10 SCC 274
12	X v. Union of India, (2021) 2 HCC (Del) 16
13	Virendra Khanna v. State of Karnataka, 2021 SCC OnLineKar 5032 (1)
14	Aaradhya Bachchan v. Bollywood Time, (2023) 6 HCC (Del) 727
15	Just Rights for Children Alliance v. S. Harish, 2024 SCC OnLine SC 2611
16	Editors Guild of India Vs. Union of India and Others 2024 SCC OnLine SC 1537
17	Apoorva Arora v. State (NCT of Delhi), (2024) 6 SCC 181
18	Jit Vinayak Arolkar v. State of Goa, 2025 SCC
19	Hemant Vs State of Haryana 2025 SCC Online P& H 16574
20	Maksud Sheikh Gaffur Sheikh v. State of Maharashtra, 2025 SCC OnLineBom 2151
21	Chandrabhan Sudam Sanap v. State of Maharashtra, (2025) 7 SCC 401

****