

10. Information technology (Amendment) act 2008

Objectives of the Act

- To grant legal recognition for transaction carried out by means of any electronic data interchange and other means of electronic communication commonly referred to as “electronic commerce” in place of paper based methods of communication.
- To give legal recognition to digital signatures for authentication of any information or matter which requires authentication under any law.
- To facilitate electronic filing of documents with government departments.
- To facilitate electronic storage of data.
- To facilitate and give legal sanction to electronic fund transfers between banks and financial institution.
- To give legal recognition for keeping of books of accounts by banker’s in electronic form.
- To amend the Indian Penal code, the Indian evidence act, 1872, The Banker’s Book evidence Act, 1891, and the Reserve Bank of India act, 1934.

Information Technology Act

- Refer Practice manual 1st question for easy and Exam oriented contents.

Digital Signature and electronic Signature (Section 3)

- The digital signature is created in two distinct steps. First the electronic record is converted into message digest by using a mathematical function known as “hash function” which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature. Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key.
- **Hash Function:** means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as “hash result” such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible.

Electronic Signature (Section 3A)

- **(1)** Notwithstanding anything contained in definition of digital signature, but subject to the provision of section (2) a subscriber may authenticate any electronic record by such electronic signature or electronic authentication techniques which-
 - a. Is considered reliable; and
 - b. May be specified in the second schedule.
- **(2)** For the purpose of this electronic signature or electronic authentication technique shall be considered reliable if,
 - a. The signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and of no other person.
 - b. the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;
 - c. any relation to the electronic signature made after affixing such signature is detectable
 - d. any alteration to the information made after its authentication by electronic signature is detectable; and
 - e. it fulfills such other conditions which may be prescribed.

Electronic Governance (Chapter III)

- **Section 4** states that where any law requires that any information or matter should be in the typewritten or printed form then such requirement shall be deemed to be satisfied if it is in an electronic form.
- **Section 5** states that where any law requires that any information or matter should be authenticated by affixing the signature of any person, then such requirement shall be satisfied if authenticated by means of digital signature affixed in such manner as may be prescribed by the central government.
- **Section 6** lays down the foundation of electronic governance. It provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in government offices and its agencies may be done through the means of electronic form. The appropriate government office has the power to prescribe the manner and format of the electronic records and the method of payment of fee in that connection.
- **Section 7** provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the following conditions are satisfied
 - a. The information therein remains accessible so as to be usable subsequently.
 - b. The electronic record is retained in its original format or in a format which accurately represents the information contained.
 - c. The details which will facilitate the identification of the origin, destination, dates and time dispatch or receipt of such electronic record are available therein.
- **Section 8** provides for the publication of any rules, regulation and notification in the electronic Gazette. It provides that where in gazette published in any form or manner then it is also deemed to be published in electronic form also. It also provides where the official gazette is published both in printed as well as in the electronic form, the date of publication shall be the date of publication of official gazette which was first published in any form.
- **Section 9** provides that the condition stipulated in sections 6, 7, and 8 shall not confer any right to insist that the document should be accepted in an electronic form by any ministry or department of the central or state government.
- **Section 10A** states that where in a contract information, the communication of proposals, the acceptance of proposals, the revocation of proposal and acceptances, as the case may be, are expressed in electronic form by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

Attribution, Acknowledgement and Dispatch of Electronic Records (Chapter IV)

- **Section 11:** an electronic record shall be attributed to the originator
 - a. If it was sent by the originator himself,
 - b. By a person who had the authority to act on behalf of the originator on respect of that electronic record; or
 - c. By an information system programmed by or on behalf of the originator to operate automatically.
- **Section 13** provides for the manner in which the time and place of dispatch and receipt of electronic records sent by the originator shall be identified. It is provided that in general, an electronic record is deemed to be dispatched at the place where the originator has his place of business and received where the addressee has his place of business.

Secure Electronic Records and Secure Electronic Signatures (Chapter V)

- **Section 14** provides where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

- **Section 15** proviso that an electronic signature shall be deemed to be a secure electronic signature if-
 - a. the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
 - b. the signature creation data was stored and affixed in such exclusive manner as may be prescribed.
- **Section 16** provides for the power of CG to prescribe any security procedure in respect of secure electronic records and secure digital signatures.

Regulation of Certifying Authorities (Chapter VI)

- Section 17 provide for appointment of controller and other officers
- Section 18 provides for the work perform by controller
- Section 19 is for recognition of foreign certifying authorities
- Section 21 is for License to issue electronic signature certificate
- Section 22 deals with Application for obtaining above license
- Section 23 deals with the renewal of license
- Section 24 is related with the procedures for grant or rejection of license
- Section 25 deals with the suspension of license.
- Section 26 deals with the notice of suspension or revocation of license
- Section 30 deals with the Duties of certifying authority. Which are as follow
 - a. Make use of hardware, software, and procedures that are secure from intrusion and misuse;
 - b. Provide a reasonable level or reliability in its services which are reasonably suited to the performance of intended function;
 - c. Adhere to security procedures to ensure that the secrecy and privacy of the electronic signature are assured
 - d. Observe such other standard as may be specified by regulation
- Section 31 deals with the compliance of act by certifying authority.
- Section 32 deals with the display of license at its business place.
- Section 33 deals with the surrender of licenses
- Section 34 deals with the disclosure regarding such act.

Electronic Signature Certificate (Chapter VII)

- **Section 35** lays down the procedures for issuance of a digital signature certificate. The fee for such application should not exceed Rs. 25,000. The section also provides that no digital signature Certificate shall be granted unless that certifying Authority satisfies that –
 - a. the applicant holds the private key corresponding to the public key to be listed in the DSC.
 - b. the applicant holds a private key, which is capable of creating a digital signature.
 - c. The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant.
- No application is rejected unless the applicant has been given a reasonable opportunity for showing cause against the proposed rejection.
- **Section 35** required that while issuing a DSC, the certifying authority should certify that it has complied that it has complied with the provision of Act, the rules and regulations made there under and also with other conditions mentioned in the DSC.
- **Section 37** deals with the suspension of DSC if it is in a public interest. A DSC shall not be suspended for a period exceeding 15 days unless the subscriber has given an opportunity of being heard in the matter.
- **Section 38** provides for the revocation of DSC under certain circumstances. The described circumstances are as follows:

- a. where the subscriber or any other person authorized by him makes a request to that effect; or
 - b. upon the death of the subscriber; or
 - c. upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.
- **Section 39** states that if suspension or revocation of DSC done through section 37 or 38 then it has to give a notice.

Duties of Subscribers (Chapter VIII)

- **Section 40** deals with the generating a Key pair. It states that where any DSC, the public key of which corresponds to the private key of that subscriber which is to be listed in the digital signature certificate has been accepted by a subscriber, the subscriber shall generate that key pair by applying security procedure.
- **Section 41** deals with the Acceptance of DSC. It states that:
 - a. a subscriber shall be deemed to have accepted a DSC if he publishes or authorizes the publication of a DSC –
 - 1. to one or more persons;
 - 2. in a responsibility, or otherwise demonstrates his approval of the DSC in any manner.
 - b. By accepting a DSC the subscriber certifies to all who reasonably rely on the information contained in the DSC that-
 - 1. The subscriber holds the private key corresponding to the public key listed in the DSC and is entitled to hold the same.
 - 2. All representations made by the subscriber to the certifying authority and all material elements to the information contained in the DSC are true;
 - 3. All information in the DSC that is within the knowledge of the subscriber is true.
- **Section 42** deals with the control of private key. The subscriber shall exercise all reasonable care to retain control of his private key corresponding to the public key. If such private key has been compromised, the subscriber must immediately communicate the fact to the certifying authority.

Penalties and Adjudication (Chapter IX)

- **Section 43** states that if any person doing damage to the system or doing the work without permission of owner or any other person who is in-charge of computer then he is liable to pay damages by way of compensation to the person so affected.
- Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.
- **Section 44** deals with the penalty to the person if he fails to furnish information, return etc. which is required under this act.
- **Section 45** provides for residuary penalty. Whoever contravenes any rules or regulations made under this act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding 25,000 rupees to the person affected by such contravention or penalty not exceeding 25,000 rupees.
- **Section 46** confers the power to adjudicate contravention under the act to an officer not below the rank of a director to the government of India or an equivalent officer of a state government.

- **Section 47** provides that while deciding upon the quantum of compensation, the adjudicating officer shall have due regard to the amount of gain of unfair advantage and the amount of loss cause to any person as well as the respective nature of the default.

Offences (Chapter XI)

Section	Description of offences	Punishment	Fine
65	Tampering with computer source documents	3 Years	2,00,000
66	Computer related offences	3 Years	1,00,000
66A	Sending offensive messages through communicating services etc.	3 Years	1,00,000
66B	Dishonestly receiving stolen computer resource or communication device	3 Years	1,00,000
66C	Identity theft	3 Years	1,00,000
66D	Cheating by personating by using computer resource	3 Years	1,00,000
66E	Violation of privacy	3 Years	1,00,000
66F	Cyber terrorism	Lifetime	-
67	Publishing or transmitting obscene material in electronic form	3 Years	5,00,000
	If above offence is subsequent time than	5 Years	10,00,000
67A	Publishing or transmitting of material containing sexually explicit act, etc.	5 Years	10,00,000
	If above offence is subsequent time than	7 Years	10,00,000
67B	Publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form	5 Years	10,00,000
	If above offence is subsequent time than	7 Years	10,00,000
67C	Prevention and retention of information by intermediaries	3 Years	2,00,000
68	Fails to comply with intentionally or knowingly and order of act	<2 Years	<1,00,000
69	Powers to issue directions for interception or decryption of any information through any computer resource	7 Years	
69A	Power to issue direction for blocking for public access of any information through any computer resource	7 Years	
69B	Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security	3 Years	
70	Attempts to secure access computer to a protected system	10 Years	
71	Penalty for misrepresentation	2 Years	1,00,000
72	Breach of confidentiality and privacy	2 Years	1,00,000
72A	Disclosure of information in breach of lawful contract	3 Years	5,00,000
73	Publishing electronic signature certificate false in certain particulars	2 Years	1,00,000
74	Publication for fraudulent purpose	2 Years	1,00,000
75	Act to apply for offence or contravention committed outside India		