

INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

Note: All the answers have been modified in the light of IT (Amendment) Act, 2008.

Question 1

Define the following terms related to Information Technology Act, 2008: (5 Marks) (May 2010)

- (i) *Computer contaminant*
- (ii) *Cyber cafe*
- (iii) *Electronic form*
- (iv) *Traffic data*
- (v) *Asymmetric crypto system.*

Answer

- (i) **Computer Contaminant:** It refers to any set of computer instructions that are designed:
 - “ to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or
 - “ by any means to disrupt the normal operation of the computer, computer system, or computer network.
- (ii) **Cyber Cafe:** It refers to any facility from where access to the Internet is offered by any person in the ordinary course of business to the members of the public.
- (iii) **Electronic Form:** It refers to any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.
- (iv) **Traffic Data:** It refers to any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data size, duration or type of underlying service or any other information.

- (v) **Asymmetric crypto system:** It refers to a system of secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

Question 2

What are the conditions subject to which electronic record may be authenticated by means of affixing digital signature? (5 Marks) (Jun 2009)

or

How does the Information Technology Act, 2008 enable the authentication of records using digital signatures? (5 Marks) (Nov 2009)

or

Write Short note on Authentication of electronic records in Information Technology (Amended) Act 2008. (4 Marks) (May 2011)

Answer

Chapter-II of IT (Amendment) Act, 2008 gives legal recognition to electronic records and digital signatures. Section 3 throws light on these conditions.

[Section 3] Authentication of Electronic Records:

- (1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.
- (2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation -

For the purposes of this sub-section, "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

- (a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
- (b) that two electronic records can produce the same hash result using the algorithm.
- (3) Any person by the use of a public key of the subscriber can verify the electronic record.
- (4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Question 3

How does the Information Technology Act, 2008 enable the objective of the Government in spreading e-governance?
(5 Marks) (Nov 2009)

Answer

Chapter III is one of the most important chapters of IT Act 2008. It deals with the procedures to be followed for sending and receiving of electronic records. This chapter contains sections 4 to 10.

Section 4 - This section provides for legal recognition of electronic records.

Section 5 - This section provides for legal recognition of Digital Signatures.

Section 6 –This 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.

Section 7 – This section provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained in the electronic form with the following conditions:

- (i) the information therein remains accessible so as to be usable subsequently,
- (ii) it is retained in its original format,
- (iii) the details such as origin, destination, dates and time of dispatch or receipt of such electronic record.

Section 8- It provides for the publication of rules, regulations and notifications in the Electronic Gazette.

Question 4

What does Information Technology (Amendment) Act, 2008 say about

- (i) *Attributes of Electronic Records in Section 11 and*
- (ii) *Secure Electronic Signature (Substituted vide ITAA 2008) in Section 15? (4 Marks) (Nov 2010)*

Answer

- (i) **Attributes of Electronic Records in Section 11 of Information Technology (Amendment) Act, 2008**

An electronic record shall be attributed to the originator:

- (i) if it was sent by the originator himself.

- (ii) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
- (iii) by an information system programmed by or on behalf of the originator to operate automatically.

(ii) [Section 15] Secure Electronic Signature (substituted vide ITAA 2008)

An electronic signature shall be deemed to be secure if:

- (i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
- (ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Question 5

Describe the duties of certifying authorities under Section 30 of Information Technology (Amended) Act 2008. (4 Marks) (May 2011)

Answer

Duties of Certifying Authorities-Section 30 of ITAA 2008

This section provides that every Certifying Authority shall follow certain procedures with respect of Digital Signatures as given below.

Every Certifying authority shall-

- a. make use of hardware, software and procedures that are secure from intrusion and misuse;
- b. provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;
- c. adhere to security procedures to ensure that the secrecy and privacy of the Electronic Signature are assured (Amended vide ITAA 2008) .
 - (ca) be the repository of all Electronic Signature Certificates issued under this Act (Inserted vide ITAA 2008)
 - (cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and (Inserted vide ITAA 2008)
- d. Observe such other standards as may be specified by regulations.

Question 6

Write short notes on the following:

- (a) Powers of Cyber Appellate Tribunal (5 Marks) (Nov 2008)
- (b) Section 41, ITAA 2008 – Acceptance of Digital Signature Certificate (4 Marks) (Nov 2010)

Answer**(a) [Section 58] Procedure and Powers of the Cyber Appellate Tribunal:**

- (1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.
- (2) The Cyber Appellate Tribunal shall have, for the purposes of discharging their functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely -
 - (a) summoning and enforcing the attendance of any person and examining him on oath;
 - (b) requiring the discovery and production of documents or other electronic records;
 - (c) receiving evidence on affidavits;
 - (d) issuing commissions for the examination of witnesses or documents;
 - (e) reviewing its decisions;
 - (f) dismissing an application for default or deciding it ex parte;
 - (g) any other matter which may be prescribed

Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

(b) [Section 41], ITAA 2008: Acceptance of Digital Signature Certificate

- (i) A subscriber shall be deemed to have accepted a Digital signature Certificate if he publishes or authorizes the publication of a digital signature certificate
 - (a) to one or more persons;
 - (b) in a repository or otherwise demonstrates his approval of the digital signatures certificate in any manner.
- (ii) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that:
 - (a) the subscriber holds the private key corresponding to the public key listed in the digital signature certificate and is entitled to hold the same;

- (b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true.
- (c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

Question 7

State the liabilities of companies under section 85 of IT (Amendment) Act, 2008.

(5 Marks) (Nov 2008)

Answer**[Section 85] Offences by Companies:**

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

However,

Nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation-

For the purposes of this section

- (i) "Company" means any Body Corporate and includes a Firm or other Association of individuals; and
- (ii) "Director", in relation to a firm, means a partner in the firm.