

Information Technology (Amendment) Act, 2008

Basic Concepts

1. **The Act:** In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for e-commerce in India and would have a major impact for e-businesses and the new economy in India. Therefore, it is important to understand 'what are the various perspectives of the IT Act, 2000 and what it offers?'. The Information Technology Act, 2000 also aims to provide the legal framework under which legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

This Act was amended by Information Technology Amendment Bill 2006, passed in Lok Sabha on Dec 22nd and in Rajyasbha on Dec 23rd of 2008. Information Technology (Amendment) Bill 2006 was amended by Information Technology Act Amendment Bill 2008 and in the process, the underlying Act was renamed as Information Technology (Amendment) Act 2008 i.e. referred to as ITAA 2008.

2. **Arrangement of Sections:** The Act consists of 90 sections spread over 13 chapters.

Question 1

Explain briefly the scope of the Information Technology (Amendment) Act 2008 along with the relevant definitions that are used.

Answer

Scope of the Information Technology (Amendment) Act 2008: This Act is meant for whole of India unless otherwise mentioned. It applies also to any offence or contravention there under committed outside India by any person. The Act was enforced by the Central Government from October 17, 2000.

The Act shall not apply to the following:

- A negotiable instrument as defined in Section 13 of the Negotiable Instruments Act, 1881;

10.2 Information Systems Control and Audit

- A power - of - attorney as defined in Section 1A of the Powers –of-Attorney Act, 1882.
- A trust as defined in Section 3 of the Indian Trusts Act, 1882.
- A will as defined in Section (h) of Section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called.
- Any contract for the sale or conveyance of immovable property or any interest in such property.
- Any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

The Act consists of 94 Sections spread over thirteen Chapters and four Schedules to the Act. The Schedules to the Act contain related amendments made in other Acts as outlined in the Objectives of the Act, namely, the Indian Penal code, the Indian Evidence Act, 1972, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India, 1934.

Section 2 contains some of the important terms that are defined below.

- (a) "Access" means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network.
- (b) "Addressee" - a person who is intended by the originator to receive the electronic record but does not include any intermediary.
- (c) "Affixing digital signature" - adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.
- (d) "Appropriate Government" - Central Government except in the following two cases where it means the State Government.
 - in the matters enumerated in List II of the Seventh Schedule to the Constitution.
 - relating to any state law enacted under List III of the Seventh Schedule to the Constitution.
- (e) "Asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.
- (f) "Computer" - any electronic, magnetic or optical or other high speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.
- (g) "Computer network" - The interconnection of one or more, computers through
 - (i) the use of satellite, microwave, terrestrial line or other communication media and

- (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.
- (h) "*Computer resource*" - computer, computer system, computer network, data, computer data base or software.
- (i) "*Computer system*" - a device or collection of devices including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions.
- (j) "*Data*" - a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.
- (k) "*Digital signature*"- authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3.
- (l) "*Electronic form*" with reference to information means any information generated , sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.
- (m) "*Electronic record*"- data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.
- (n) "*Function*" - in relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer.
- (o) "*Information*" includes data, text, images, sound, voice, codes, computer programs, software and databases or micro film or computer generated micro fiche.
- (p) "*Intermediary*" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.
- (q) "*Key pair*", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.
- (r) "*Originator*" - a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.
- (s) "*Prescribed*"- prescribed by rules made under this Act.

10.4 Information Systems Control and Audit

- (t) *"Private key"* - the key of a key pair used to create a digital signature.
- (u) *"Public key"* - the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.
- (v) *"Secure system"* means computer hardware, software and procedure that
 - are reasonably secure from unauthorized access and misuse.
 - provide a reasonable level of reliability and correct operation.
 - are reasonably suited to performing the intended function and
 - adhere to generally accepted security procedures.
- (w) *"Verify"* - in relation to a digital signature electronic record on public key with its grammatical variations and cognate expressions means to determine whether
 - the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber.
 - the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

Question 2

Define the following terms with reference to section 2 of Information Technology (Amendment) Act 2008:

- (i) *Digital signature*
- (ii) *Electronic form*
- (iii) *Key pair*
- (iv) *Asymmetric crypto system*
- (v) *Adjudicating officer.*

Answer

- (i) **Digital Signature:** It is a authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3:
- (ii) **Electronic form:** It is reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated micro fiche or similar device.
- (iii) **Key Pair:** It is an asymmetric cryptosystem, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.
- (iv) **Asymmetric crypto system:** It is 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.

- (v) **Adjudicating Officer:** It means an adjudicating Officer appointed under sub-section (1) of section 46.

Question 3

What are the conditions subject to which electronic record may be authenticated by means of affixing digital signature?

Answer

Chapter-II of Information Technology (Amendment) Act 2008 gives legal recognition to electronic records and digital signatures. It contains only **section 3**.

This Section deals with the conditions subject to which an electronic record may be authenticated by means of affixing digital signature which is created in two definite steps. First the electronic record is converted into a 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 any body who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

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- to derive or reconstruct the original electronic record from the hash result produced by the algorithm; that two electronic records can produce the same hash result using the algorithm.

Question 4

How does the Information Technology (Amendment) Act 2008 enable the authentication of records using digital signatures?

Answer

Chapter-II, Section 3 of Information Technology (Amendment) Act 2008 provides conditions subject to which an electronic record is authenticated by means of affixing digital signature.

- The digital signature is created in two distinct steps. First the electronic record is converted into a 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.

10.6 Information Systems Control and Audit

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 corresponding public key.

This will enable anybody to verify whether the electronic record is retained intact or has been tampered with; since it was fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

Question 5

How does the Information Technology (Amendment) Act 2008 enable the objective of the Government in spreading e-governance?

Answer

In Information Technology (Amendment) Act 2008, chapter III is related with the objective of the government in spreading e-governance. 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 the legal recognition of electronic records.

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

Section 6 – It 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 6

Discuss the main provisions provided in Information Technology (Amendment) Act 2008 to facilitate E-governance.

Answer

E-Governance sections of chapter III 6, 7 and 8 are the main sections for provisions related to E-governance provided in Information Technology (Amendment) Act 2008 to facilitate e-governance.

Section 6 lays down the foundation of electronic Governance. It provides that the filling of any form, application or other documents; creation, retention or preservation of records, issue or grant of any license or permit; receipt or payment in Government offices and its agencies may be done by means of electronic form. The appropriate Government 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 has to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form under the following conditions:

- (i) The information therein remains accessible so as to be usable subsequently.
- (ii) The electronic record is retained in its original format or in a format which accurately represents the information contained.
- (iii) The details which will facilitate the identification of the origin, destinations, dates and time of dispatch or receipt of such electronic record to be dispatched or received.

This section does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received. Moreover this section does not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Section 8 provides for the publication of rules, regulations, order, bye-law and notifications in the official Gazette in an electronic form. It provides that where any law requires the publication of any rule regulation, order, bye law, notification or any other matter in the Official Gazette, both in the printed as well as in the electronic form, the date of publication shall be the date of publication of the Official Gazette which was first published in any form.

Question 7

What are the regulations relating to the appointment and powers of the certifying authorities under Chapter VI, Section 17 to 25 of Information Technology (Amendment) Act 2008?

Answer**Regulation of Certifying Authorities [Chapter VI – Section 17–25]:**

Chapter VI contains detailed provisions relating to the appointment and powers of the Controller and Certifying Authorities.

Section 17 provides for the appointment of Controller and other officers to regulates the Certifying Authorities.

10.8 Information Systems Control and Audit

Section 18 lays down the functions which the controller may perform in respect of activities of Certifying Authorities.

Section 19 provides for the power of the Controller with the previous approval of the Central Government to grant recognition to foreign certifying Authorities subject to such conditions and restrictions as may be imposed by regulations.

Section 20 This Section provides that the controller shall be acting as repository of all Digital Signature Certificates issued under the Act. He shall also adhere to certain security procedure to ensure secrecy and privacy of the digital signatures and also to satisfy such other standards as may be prescribed by the Central Government. He shall maintain a computerized database of all public keys in such a manner that they are available to the general public.

Section 21 This section provides that a license to be issued to a certifying authority to issue digital signature certificates by the controller shall be in such form and shall be accompanied with such fees and other documents as may be prescribed by the Central Government. Further, the Controller after considering the application may either grant the licence or reject the application after giving reasonable opportunity of being heard.

Section 22 This Section provides that the application for license shall be accompanied by a certification practice statement and statement including the procedures with respect to identification of the applicant. It shall be future accompanied by a fee not exceeding Rs. 25,000 and other documents as may be prescribed by the Central Government.

Section 23 provides that the application for renewal of a license shall be in such form and accompanied by such fees not exceeding Rs. 5,000 which may be prescribed by the Central Government.

Section 24 deals with the procedure for grant or rejection of license by the Controller on certain grounds.

No application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

Section 25 provides that the controller may revoke a licence on grounds such as incorrect or false material particulars being mentioned in the application and also on the ground of contravention of any provisions of the Act, rule, regulation or order made there under.

Question 8

What are the duties of a certifying authority under Section 30 of the Information Technology (Amendment) Act 2008?

Answer

Duties of Certifying Authorities {Section 30}:

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

- (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 digital signatures are assured and
- (d) Observe such other standards as may be specified by regulations.

Question 9

What is a Digital Signature? How is it used? What are the duties of certifying authorities in regard to its usage?

Answer

Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure.

The digital signature is created in two distinct steps. First the electronic record is converted into a 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 of the contents of the electronic record will immediately invalidate the digital signature. Secondly, the identification of the person affixing the digital signature is authenticated through the use of the 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. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

Section 5 of Chapter III provides for legal recognition of Digital Signatures where any law requires that any information or document should be authenticated by affixing the signature of any person, then such a requirement can be satisfied if it is authenticated by means of Digital Signatures affixed in such manner as may be prescribed by the Central Government.

Duties of Certifying Authority:

1. According to Section 30 of the Information Technology (Amendment) Act 2008, Certifying Authority shall follow certain procedures in respect of Digital Signatures as given below:
 - Make use of hardware, software and procedures that are secure from intrusion and misuse.
 - Provide a reasonable level of reliability in its services, which are reasonably suited to the performance of intended functions.
 - Adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured and
 - Observe such other standards, as specified by the regulation.

10.10 Information Systems Control and Audit

2. Every Certifying Authority shall ensure that every person employed by him complies with the provisions of the Act, or rules, regulations or orders made there under.
3. A Certifying Authority must display its licence at a conspicuous place of the premises in which it carries on its business. A Certifying Authority whose licence is suspended or revoked shall immediately surrender the license to the Controller.
4. Every Certifying Authority shall display its Digital Signature Certificate, which contains the public key corresponding to the private key used by that Certifying Authority and other relevant facts.

Question 10

Write short notes on the following:

- (a) *Digital Signature Certificate*
- (b) *Encryption.*

Answer

- (a) **Digital Signature Certificate:** A digital signature certificate is a mechanism for authenticating and securing the information that is transmitted between the two parties. It is an authoritative identification about a person or a company. It is simply a public key, along with some identifying information, that has been digitally signed by a certificate authority. It identifies the subscriber, certification authority, and its operational period and contains the subscriber public key. The certificate is thus protected so that it cannot be altered without detection. It is like an electronic passport that authenticates identity of an entity. The identifying information in the certificate can be trusted because the digital signature is cryptically strong.

Legal recognition of digital signature, electronic records and authentication is necessary in an electronically formed contract. The Information Technology Act provides legal status on the use of the electronic records and signatures. Authentication and non-repudiation are secured through the mechanism of digital signature. The digital signature certificate ensures that the purported sender is in fact the person who sent the message. By certifying that a particular public key does indeed belong to a specific person, it authenticates and makes digital signature conclusive. For verification of such signature, the verifier must have the signer's public key and have an assurance that it corresponds to his private key. Digital certificate associates a particular person to that pair. Its basic purpose is to serve the need of the person seeking to verify a digital signature who would want to know that:

- The public key corresponds to the private key used to create the digital signature;
- Whether the public key is identified with the signer.

Section 35 of the Act deals with the issue of the digital certificate by the Certifying Authority, on an application being made in the prescribed form.

- (b) **Encryption:** Encryption refers to conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm to convert the original message called clear text into a coded equivalent called cipher text. At the receiving end, the cipher text is decoded (decrypted) back into clear text. The encryption algorithm uses a key, which is a binary number that is typically from 56 to 128 bits in length. The more bits in the key, the stronger the encryption method. Today, nothing less than 128 bit algorithms are considered truly secure. Two general approaches to encryption are private key and public key encryption.

Private Key Encryption: Data encryption standard (DES) is a private-key encryption technique designed in the early 1970s by IBM. The DES algorithm uses a single key known to both the sender and the receiver of the message. To encode a message, the sender provides the encryption algorithm with the key, which is used to produce a cipher text message. The message enters the communication channel and is transmitted to the receiver's location, where it is stored. The receiver decodes the message with a decryption program that uses the same key employed by the sender.

Public Key Encryption: The public key encryption technique uses two different keys: one for encoding messages and the other for decoding them. Each recipient has a private key that is kept secret and a public key that is published. The sender of a message uses the receiver's public key to encrypt the message. The receiver then uses his or her private key to decrypt the message. Users never need to share their private keys to decrypt messages, thus reducing the likelihood that it may fall into the hands of criminal.

Question 11

State the duties of the subscriber of a digital signature as specified in Section 40 to 42 of Chapter VIII of Information Technology (Amendment) Act 2008.

Answer

The duties of the subscriber of a Digital Signature as specified in Section 40 to 42 of Chapter VII of Information Technology (Amendment) Act 2008 are as follows:

On acceptance of the Digital Signature Certificate the subscriber shall generate a key pair using a secure system.

A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate-

- (i) to one or more persons;
- (ii) in a repository, or otherwise demonstrates his approval of the Digital Signature
- (iii) certificate in any manner.

By accepting a Digital Signature Certificate, the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that –

10.12 Information Systems Control and Audit

- (i) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
- (ii) all representations made by the subscriber to the Certificate Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
- (iii) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

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 (i.e., endangered or exposed), the subscriber must immediately communicate the fact to the Certifying Authority.

Otherwise, the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

Question 12

Explain with reference to "Information Technology (Amendment) Act 2008":

- (i) *Penal Provisions*
- (ii) *Electronic Governance*

Answer

- (i) **Penal Provisions:** Chapter IX contains sections 43 to 47. It provides for awarding compensation or damages for certain types of computer frauds. It also provides for the appointment of Adjudication Officer for holding an inquiry in relation to certain computer crimes and for awarding compensation. Sections 43 to 45 deal with different nature of penalties.

Penalty for damage to computer, computer system or network: Section 43 deals with penalty for damage to computer, computer system, etc by any of the following methods:

- (a) securing access to the computer, computer system or computer network;
- (b) downloading or extracting any data, computer database or information from such computer system or those stored in any removable storage medium;
- (c) introducing any computer contaminant or computer virus into any computer, computer system or network;
- (d) damaging any computer, computer system or network or any computer data, database or programme;
- (e) disrupting any computer, computer system or network;
- (f) denying access to any person authorized to access any computer, computer system or network;
- (g) providing assistance to any person to access any computer, computer system or network in contravention of any provisions of this Act or its Rules;

- (h) charging the services availed of by one person to the account of another person by tampering with or manipulation any computer, computer system or network.

Explanation.- For the purposes of this section,-

- (i) “computer contaminant” means any set of computer instructions that are designed:
 - (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
 - (b) by any means to disrupt the normal operation of the computer, computer system, or computer network;
- (ii) “computer database” means a representation or information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
- (iii) “computer virus” means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
- (iv) “damage” means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

Section 44 states that if any person who is required under this Act or any rules or regulations made there under to:

- (a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
- (b) file any return or furnish any information, books or other documents within the time specified in the regulations fails to file, return or furnish the same within the time specified in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;
- (c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

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

10.14 Information Systems Control and Audit

twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Section 46 confers the power to adjudicate contravention under the Act to an officer not below than the rank of a Director to the Government of India or an equivalent officer of a State Government. Such appointment shall be made by the Central Government. In order to be eligible for appointment as an adjudicating officer, a person must possess adequate experience in the field of Information Technology and such legal or judicial experience as may be prescribed by the Central Government. The adjudicating officer so appointed shall be responsible for holding an inquiry in the prescribed manner after giving reasonable opportunity of being heard and thereafter, imposing penalty where required.

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 caused to any person as well as the respective nature of the default.

- (ii) **Electronic Governance:** It specifies the procedures to be followed for sending and receiving of electronic records and the time and the place of the dispatch and receipt.

Section 4 provides for "legal recognition of electronic records". It provides 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 provides for legal recognition of Digital Signatures. 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 it is authenticated by means of Digital Signatures affixed in such manner as may be prescribed by the Central Government.

For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

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 licence 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:

- (i) the information therein remains accessible so as to be usable subsequently.

- (ii) The electronic record is retained in its original format or in a format which accurately represents the information contained.
- (ii) The details which will facilitate the identification of the origin, destination, dates and time of despatch or receipt of such electronic record are available therein.

This section does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

Moreover, this section does not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Section 8 provides for the publication of rules, regulations and notifications in the Electronic Gazette. It provides that where any law requires the publication of any rule, regulation, order, bye-law, notification or any other matter in the Official Gazette, then such requirement shall be deemed to be satisfied if the same is published in an electronic form. It also provides where the Official Gazette is published both in the printed as well as in the electronic form, the date of publication shall be the date of publication of the Official Gazette which was first published in any form.

Question 13

Describe the composition and powers of Cyber regulatory appellate tribunal.

Answer

Cyber Regulatory Appellate Tribunal: The cyber regulation appellate tribunal shall consist of one person only called the Presiding Officer of the Tribunal who shall be appointed by the Central Government. The person must be qualified to be a Judge of a High Court or is or has been a member of Indian Legal Services in the post in Grade I of that service for at least three years. The Presiding Officer shall hold the office for a term of five years or upto a maximum age limit of 65 years, whichever is earlier.

Some of the powers specified are following:

- (i) Summoning and enforcing the attendance of any person and examining him on oath.
- (ii) Requiring production of documents and other electronic records.
- (iii) Receiving evidence on affidavits
- (iv) Reviewing its decisions.
- (v) Issuing commissions for examination of witness etc.

Question 14

Write short notes on the Powers of Cyber Appellate Tribunal.

Answer

Powers of Cyber Appellate Tribunal: Section 58 provides for the procedure and powers of the Cyber Appellate Tribunal. The Tribunal shall also have the powers of the Civil Court under

10.16 Information Systems Control and Audit

the Code of Civil Procedure, 1908. Some of the powers specified are in respect of the following matters:

- (i) summoning and enforcing the attendance of any person and examining him on oath;
- (ii) requiring the discovery and production of documents or other electronic records;
- (iii) receiving evidence on affidavits;
- (iv) issuing commissions for the examination of witnesses or documents;
- (v) reviewing its decisions;
- (vi) dismissing an application for default or deciding it ex-parte;
- (vii) any other matter which may be prescribed.

The appellant may either appear in person or may be represented by a legal practitioner to present his case before the Tribunal.

Question 15

State the liabilities of companies under section 85 of Information Technology (Amendment) Act 2008.

Answer

Liability of Companies under Section 85 of Information Technology (Amendment) Act, 2008: Where a company commits any offence under this Act or any rule there under, every person who, at the time of the contravention, was in charge of and was responsible for the conduct of the business of the company shall be guilty of the contravention. However, he shall not be liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent the contravention.

Further, where a contravention has been committed by a company, and it is proved that the contravention took place with the connivance or consent of or due to any negligence on the part of any director, manager, secretary or other officer of the company, such officer shall be deemed to be guilty and shall be liable to be proceeded against and punished accordingly.

For the purposes of this section, 'company' includes a firm or other association of persons and 'director' in relation to a firm means a partner in the firm.

The Information Technology Act will go a long way in facilitating and regulating electronic commerce. It has provided a legal framework for smooth conduct of e-commerce. It has tackled the following legal issues associated with e-commerce:

- Requirement of writing
- Requirement of a document
- Requirement of a signature and
- Requirement of legal recognition for electronic messages,
- Records and documents to be admitted in evidence in a court of law.

Question 16

Please read carefully the following three scenarios and answer the questions given below:

(a) **Scenario 1:**

Nobody told you that your Internet use in the office was being monitored. Now you have been warned you will be fired if you use the Internet for recreational surfing again. What are your rights?

(b) **Scenario 2:**

Your employees are abusing their Internet privileges, but you don't have an Internet usage policy. What do you do?

(c) **Scenario 3:**

Employee Mr. X downloads adult material to his PC at work, and employee Miss Y sees it. Miss Y then proceeds to sue the company for sexual harassment. As the employer, are you liable?

Answer

- (a) **Scenario 1:** When you are using your office computer, you have virtually no rights. You would have a tough time convincing the court that the boss invaded your privacy by monitoring your use of the company PC during office hours. You should probably be grateful that you only got a warning stating that you will be fired if you use the Internet for recreational surfing again.
- (b) **Scenario 2:** Although the law is not fully developed in this area, courts are taking a straightforward approach. If it is a company computer, the company can control the way in which it is to be used by its employees. You really don't need an Internet usage policy to prevent inappropriate use of your company's computer. To protect the company in future, it is advisable to distribute an Internet usage policy to your employees as soon as possible to stop your employees from abusing their Internet privileges.
- (c) **Scenario 3:** Whether it comes from the Internet or from a magazine, adult material simply has no place in the office. So Miss Y could certainly sue the company for making her work in a sexually hostile environment. The best defense for the company is to have an Internet usage policy that prohibits employees to access adult sites. Of course, you have to follow-through and monitor. Today, software is available for monitoring the employees whenever they visit adult sites. It will shut down the computer and alert the person who is monitoring Internet usage. If someone is caught browsing adult material in the office, you must at least send a written communication to the offending employee. If the company lacks a strict Internet usage policy, Miss Y could prevail in the Court.

Exercise

Question 1

What are the major objectives of Information Technology (Amendment) Act 2008? Explain in brief.

Question 2

Briefly explain the power of central government to make rules with respect to the Section 10 of Information Technology (Amendment) Act 2008.

Question 3

Explain the power of Controller to make regulations under Section 89 of the Information Technology (Amendment) Act 2008.

Question 4

What are the powers of a Police Officer under the Information Technology (Amendment) Act 2008 to enter and search etc?

Question 5

Define 'Electronic Signature' and 'Electronic Signature Certificate' in the light of the Information Technology (Amendment) Act 2008.

Question 6

Briefly explain the Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form as per Section 67 A of the Information Technology (Amendment) Act 2008.