CNS Assignment

LUBNA.N
IBG17I3023

MODULE 5

1) Give the aim and objectives of the IT Act, 2000.

- To give legal recognition to transactions done by electronic way or by use of the internet.
- To grant legal recognition to digital signature for accepting any agreement via computer.
- To provide facility of filling documents online
- To authorize any undertaking to store their data in electronic storage.
- To prevent cyber crime by imposing high penalty for such crimes and protect privacy of internet users.
- To give legal recognition for keeping books of account by bankers and other undertakings in electronic form.

---

2) What are the important provisions of the IT Act, 2000

The important provisions are :

a) Digital Signature : Authentication of Electronic Records

b) Electronic Governance : Legal Recognition of Electronic Records

c) Electronic Governance : Legal Recognition of Digital Signatures

d) Use of Electronic Records and Digital Signatures in Government and Its Agencies

e) Retention of Electronic Records

f) Publication of Rules and Regulations in the Electronic Gazette

g) Power to Make Rules by central Government in Respect of Digital Signatures.

3) Who is a Controller? Outline his functions and powers

The Controller will act as a repository of all digital signature certificates under this Act.

Makes use of secure hardware, software and also procedures and ensures the security of digital signatures

Functions of a Controller:-

i) exercising supervision over the activities of the Certifying Authorities

ii) certifying public keys of the Certifying Authorities

iii) laying down the standards to be maintained by the Certifying Authorities.

iv) specifying the qualifications and experience that which employees of the Certifying Authorities should possess.

v) specifying the conditions subject to which the Certifying Authorities shall conduct their business

vi) specifying the contents of written, printed or visual materials and advertisements that may be distributed

vii) Resolving any conflict of interest between the Certifying Authorities and the subscribers

viii) laying down the duties of the certifying Authorities.

---

4) Describe the duties of subscribers.

i) Generating key pair

Where any Digital Signature Certificate, 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 the key pair by applying the security procedure.

ii) Acceptance of Digital Signature Certificate.

a) A subscriber shall be deemed to have accepted a Digital signature certificate if he publishes or authorises the publication of a Digital Signature Certificate.

- to one or more persons
- in a repository

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

- subscriber holds the private key corresponding to public key listed in Digital Signature Certificate.
- all representations made by the subscriber to the Certifying authority
- all information in the Digital Certificate.

iii) Control of Private key.

a) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to public key.

b) If the private key corresponding to public key listed in the digital signature certificate has been compromised the subscriber shall communicate this without delay to the Certifying Authority.

5) List the offences with reference to computer system

- Tampering with computer source Documents
- Hacking with computer system
- Punishment for receiving stolen Computer Resource or Communication Device.
- Punishment for Identity Theft
- Punishment for cheating by Personation by Using Computer Resource.
- Punishment for Violation of Privacy
- Punishment for Cyber Terrorism
- Punishment of Information which is obscene in Electronic Form
- Punishment for Publishing or Transmitting of Material Containing sexually Explicit Act in Electronic Form.
- Power of Controller to Give Directions
- Government's Agency Power to Intercept Information
- Protected System
- Penalty for Misrepresentation
- Penalty for Breach of Confidentiality and Privacy.
- Penalty for Publishing Digital Signature Certificate False in Certain Particulars
- Publication for fraudulent purpose
- Act to Apply for Offence or Contravention Committed Outside India
- Confiscation

- Penalties or Confiscation Not to Interfere with other Punishments.
- Power to Investigate Offences.

---

6) When network service provider's not be liable under IT Act. Explain.

No person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him, if he proves that the offence or contravention was committed without his knowledge.

- Network Service provider means an intermediary
- third party information means any information dealt with by a network service provider in his capacity as an intermediary.

---

7) What are the miscellaneous provisions of IT Act ? Explain

- Power of Police Officer and other Officers to Enter, search.
- Act to Have Overriding Effect
- Controller, Deputy Controller and Assistant Controllers to Be Public Servants
- Power to Give Directions
- Protection of Action Taken in Good faith
- Offences by Companies
- Removal of Difficulties.

- Constitution of Advisory committee
- Special Provisions for Evidence Relating to Electronic record
- Admissibility of Electronic Records
- Presumption As to Electronic Records and Digital Signatures
- Presumption As to Digital Signature Certificates
- Presumption As to Electronic Messages.

---

8) Explain the following

a) Secure electronic record

When any security procedure has been applied to an electronic record at a specific point of time, then such a record shall be deemed to be a secure electronic record from a such a point of time to the time of verification.

b) Secure Digital Signature.

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time was affixed, was

- unique to the subscriber affixing it
- capable of identifying such a subscriber
- created in a manner or using a means under the exclusive control of the subscriber

c) Certifying authority, suspensions and revocations of digital signature.

Certifying authority

- Any ~~authority~~ person may make an application to the CA for the issue of a Digital Certificate Signature.
- Every such application shall be accompanied by a fee not exceeding 25,000 ₹ as prescribed by Central Government
- Each such application shall be accompanied by a certification practice statement

Suspension of DSC.

- subject to the provisions of IT Act, the CA which had issued a Digital Signature Certificate may suspend
  - on receipt of a request to that effect from the subscriber or any person who is duly authorized
- A DSC shall not be suspended for a period exceeding 15 days unless the subscriber has given opportunity.

Revocation of DSC

A CA may revoke a DSC issued by it,

- where the subscriber, or any other person authorised by him, makes a request to that effect
- upon death of subscriber
- upon dissolution of the firm.

---

a) Briefly explain penalties and adjudications in IT Act.

a) Penalty for Damage to Computer, Computer System

If any person without the permission of the owner or any other person who is in charg of a computer,

- Accesses or secures access to such computer component
- downloads, copies or extracts any data, computer database
- introduces, or causes to be introduced, any computer contaminant or computer virus into any computer.
- disrupts, or causes disruption of any computer, computer system / network.

b) Compensation for Failure to Protect Data

If a body corporate, possessing, dealing or handling any sensitive personal data in a computer resource which it owns, controls, maintains reasonable security practices, such body corporate shall be liable to pay damages to the aggrieved party.

c) Penalty for failure to furnish Information Return

If any person who is required under this Act rule thereunder to

- furnish any document, return or report to the controller or CA, fails to furnish is liable to a penalty not exceeding 150,000 for each failure.
- file any return or furnish any info or other documents within time specified is liable to a penalty not exceeding 5000 for each day

d) Residual Penalty

Whoever contravenes any rules or regulations to which no penalty has been seperately provided is liable to pay a compensation not exceeding ₹ 25,000 to person affected.

Adjudications

- The adjudicating officer shall, after giving the person referred in IT Act reasonable for making a representation in the matter impose penalty or award such compensation if he thinks he fit in accordance with the provision
- No person shall be appointed as an adjudicating officer unless he possess required experience.

Powers

- the amount of gain or unfair advantage, where ever qualifiable made as a result of the default
- the amount of loss caused to any person as a result of the default.

---

10) Explain the process of issuing digital certificate and revocation of digital signature certificate by a certifying authority.

- Any person may make an application to the Certifying Authority for the issue of a Digital Signature certificate in such form as may be prescribed by the Central Government.
- Every such application shall be accompanied by a fee not exceeding ₹ 25000 as prescribed
- Each such application shall be accompanied by a certification practice statement or, where there is no such statement containing such particulars as specified.
- On receipt of an application, the CA may practice statement and after making such enquiries as it may deem fit grant the DC.

Revocation of DSC

i) A CA may revoke a DSC issued by it

- where the subscriber or any person authorized by him, makes a request to that effect
- upon death of subscriber
- upon dissolution of firm

ii) A DC must not be revoked unless the subscriber has been given an opportunity to be heard.

ii) Explain the various offences and punishments on cyber crime.

Offences

i) Tampering with computer System Documents.

Whoever knowingly / intentionally conceals, destroys or alters any record shall be punishable with imprisonment upto 3 years

ii) Hacking with Computer System.

If any person does this, he shall be punishable with imprisonment for a term which may extend to 3 years to 5yrs.

Punishments

a) Whoever,

a) with intent to threaten the unity of India or strike terror in people by

- denying or cause the denial of access to any person authorized to access computer
- attempting to penetrate or access a computer resource without authorization

b) knowingly or intentionally penetrates or accesses a computer resource without authorization access, to a database that is restricted commits the offence of cyber terrorism.