The Information Technology Act 2000

For Internal Circulation and Academic Purpose Only

Programme Educational Objectives

- *Our program will create graduates who:*

- *1. Will be recognized as a creative and an enterprising team leader.*
- *2. Will be a flexible, adaptable and an ethical individual.*
- *3. Will have a holistic approach to problem solving in the dynamic business environment.*

Business Legislations Course Outcomes

- CO1Given the circumstances, the learner will be able to infer legal aspects of doing business & plan business activities.

- CO2In a given situation, the learner will be able make use of provisions of the Contract Act to evaluate a contract used in commercial practice with 70% accuracy.

- CO3In a given situation, learner will be able to distinguish between various types of Companies and explain their comparative advantages and disadvantages

- CO4 The learner will be able to describe the legal process involved in formation of a company and identify the relationships amongst the various stakeholders of the company.

- CO5 When needed, the learner will be able to examine the various provisions of consumer protection act and determine steps to be taken in case of consumer related complaints.

- CO6 In a given situation, student manager will be able to make use of various legal provisions of Information Technology Act.

INTRODUCTION

- The IT act, called the Information Technology Act, 2000came into force on 17 October 2000
- The Act extends to whole of India and also to people who contravene the provisions of the act outside India.
- The Act was enacted to give legal recognition to the transactions carried out by means of electronic data exchange.

INTRODUCTION

- The IT Act enabled in the carrying out of ‘Electronic Commerce’.
- It also facilitated the filing of electronic documents to the Government agencies, by means of paperless methods of communication and storage of information.
- The law applies to any kind of information in the form of data message used in commercial activities.

Objectives of the Act

- To grant legal recognition to transactions carried on by means of electronic data exchange.
- To give legal recognition to ‘Digital Signatures’
- To help electronically filing of records.
- The help in electronic storage of data.
- To give legal recognition to transfer of funds between banks and financial institutions.
- To give legal recognition to keeping of books of accounts by bankers in electronic form.

Application of the Act

It does not apply to the following.

- A negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;
- A power-of-attorney as defined in section 1A of the Power-of-attorney Act, 1882;
- A trust as defined in section 3 of the Indian Trusts Act, 1882;
- A will as defined in section 2 (h) of the Indian Succession Act, 1925 (39 of 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.

For Internal Circulation and Academic Purpose Only

DIGITAL SIGNATURES

- In electronic massages handwritten signature are not possible.
- The law of IT recognizes the Digital Signature as electronic equivalent of the handwritten Signature.
- Sec 2 (1)(p) -"digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

DIGITAL SIGNATURES

- The Act has adopted the Public Key Infrastructure (PKI) for securing electronic transactions.
- A digital signature means an authentication of any electronic record by a subscriber by means of any electronic method or any procedure in accordance with the other provisions of the Act.
- A subscriber can authenticate an electronic record by affixing his digital signature.
- A private key is used to create a digital signature whereas a public key is used to verify the digital signature and electronic record.
- They both are unique for each subscriber and together form a functioning key pair.

Verification of Digital Signature

Verification means to determine if:

a) The initial electronic record was affixed with the digital signature

b) The initial electronic record is retained intact or has been altered after the digital signature has been affixed.

Verification – Any person by use of the public key of the subscriber can verify the electronic record' the public and private key are unique and together constitute 'a pair'

The verification means to check if:

c) The digital signature was created using the corresponding private key.

d) If the software generates same hash codes, then the document is stated to be verified.

Digital Signature Certificate

1. Any person may make an application to the Certifying authority to obtain a Digital Signature.
2. The Certifying Authority may, after making enquiries issue a Digital Signature Certificate.
3. The Digital Signature shall have a expiry date.
4. A new digital signature certificate may be issued after the expiry of the old certificate.
5. The Certifying Authority shall charge a fee for issue of such certificate as prescribed by the Central Government.
6. No Interim Digital Signature Certificate shall be issued.

Generation of Digital Signature Certificate

The Generation of Digital Signature Certificate shall involve -

1. Receipt of the request for DSC
2. Creation of a new digital certificate
3. Binding the Key pairs with the DSC.
4. Issue of DSC and the associated public key .
5. Creation of a unique name of the DSC owner

Revocation of DSC

A Certifying authority shall revoke the DSC by

1. Request from the Subscriber.
2. On death of the subscriber.
3. Dissolution & Winding up of the firm.
4. Upon any false information or misrepresentation by the subscriber
5. Upon not furnishing any required information.
6. When the reliability of the DSC has been compromised
7. The subscriber declared insolvent.
8. Upon misuse of the DSC
9. When the DSC is not required.

Powers to Central Government

The Act also gives the Central Government powers:

a) to make rules prescribing the digital signature

b) the manner in which it shall be affixed

c) the procedure to identify the person affixing the signature

d) the maintenance of integrity, security and confidentiality of records or

e) payments and rules regarding any other appropriate matters

Regulation for Certifying Authorities

- Central Government has the power to appoint Controller of Certifying Authorities
- The procedure for issuing license to “Certifying Authorities” as well as the procedure for suspension and revocation or renewal of the license has also been laid down under the IT Act.
- The Controller Shall act as a repository of the Digital Signature Certificates issued under this Act. (Sec. 20)
- The Central government shall have powers to decide upon:

a) Appointments of Controller, Deputy and Assistant Controller.

b) The qualifications, experience and terms and conditions of service

c) The location of Head office and Branch Offices

d) The Office of the Controller shall have a seal.

Duties of Certifying Authorities

- The Certifying Authorities shall have the following duties:

a) To ensure the compliance of the Act from every person employed or engaged.

b) To display its license at a conspicuous place.

c) To surrender the license immediately upon revocation.

d) To make regular disclosure of all its activities.

e) To notify the person in who has been granted the Certificate of any situation which may have an adverse effect on the certificate holder.

Duties of the Subscribers

- The IT Act has laid down the following duties of the Subscribers of the Digital Signature Certificate

a) To accept the DSC (Sec 41)

b) To generate the Key pair by applying the security procedure. (Sec 40)

c) Take reasonable care of the to retain control over the private key. (Sec 42)

d) The subscriber must take all precautions not to disclose the private key to any third party. If however, the private key is compromised, he must communicate the same to the Certifying Authority (CA) without any delay.

Objectives of the Act

- These signatures are to be authenticated by Certifying Authorities (CAs) appointed under the Act. These authorities would inter alia, have the license to issue Digital Signature Certificates (DSCs). The applicant must have a private key that can create a digital signature. This private key and the public key listed on the DSC must form the functioning key pair.

DESPATCH & ACKNOWLEDGEMENT OF ELECTRONIC RECORDS

- All electronic records sent by an originator, his agent or an information system programmed by or on his behalf are attributable to him .
- Where the originator has not agreed with the addressee that the acknowledgement of receipt of electronic data shall be given in a manner, the acknowledgement may be given by
- Any communication by the addressee, automated or otherwise; or
- Any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received

DESPATCH & ACKNOWLEDGEMENT OF ELECTRONIC RECORDS

- Where the originator had stipulated that it shall be binding only on receipt of acknowledgement, then unless acknowledgement has been received, it shall mean that the electronic data was never sent.
- Where no such stipulation was made, then the originator may give a notice to the addressee stating that no such acknowledgement has been received and specifying a time by which the acknowledgement must be received by him, if still no acknowledgement is received, he may after giving notice to the addressee treat the electronic data as never sent

Penalty for damage to computer, computer system etc.

- “Damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means
- Tampering with the computer source documents. Whoever knowingly or intentionally conceals, destroys, or alters or causes another to do the same any computer source code used for a computer, computer programme, computer system or computer network, shall be punishable with imprisonment up to three years, or with fine upto Rs. 2 lakhs or with both.

Penalty for damage to computer, computer system etc.

- Whoever commits hacking of the computer system shall be punished with imprisonment up to three years, or with fine upto Rs. 2 lakhs or with both.
- Whoever publishes or transmits or cause to be published any matter which is obscene, shall be punished on first conviction with imprisonment may extend upped five years with a fine of upped RS. 1,00,000 (for second and subsequent convictions, imprisonment of upped 10 years and a fine of upped RS. 2,00,000)

Penalty for damage to computer, computer system etc.

- The government may notify certain computer systems or networks as being "protected systems", unauthorized access to which may be punishable with imprisonment upped 10 years in addition to a fine.
- Whoever makes a misrepresentation to, or suppresses any material fact from the Controller of Certifying Authorities and whoever commits breach of confidentiality and privacy, having access to electronic data under the Act shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to RS. 1,00,000 or with both.

ADJUDICATION /COMPENSATION

- The Act provides the following:

a) Damages by way of compensation not exceeding Rs. 10 million may be imposed for unauthorized access, unauthorized downloading or copying of data, introduction of computer viruses or contaminants, disruption of systems, denial of access or tampering with or manipulating any computer/network.

b) The Act does provide that no penalty imposed under the Act shall prevent imposition of any other punishments attracted under any other law for the time being in force.

c) The provisions of the Act shall also apply to offences or contravention outside India, if such offences or contravention involves a computer, computer system or computer network located in India.

Some Explainations

- Computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video are prepared or being prepared or produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
- “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;

Some Explainations

- “Computer contaminant" means set of computer instructions designed:
  - - to modify, destroy, record, transmit data or programe residing within a computer, computer system or computer network; or
  - - by any means to usurp the normal operation of the   computer, computer system, or computer network;

CYBER REGULATIONS APPELLATE TRIBUNAL (CRAT)

- A Cyber Regulations Appellate Tribunal (CRAT) is to be set up for appeals from the order of any adjudicating officer. It consists of one person only- the Presiding Officer.
- No appeal shall lie from an order made by an adjudicating officer with the consent of the parties.
- Every appeal must be filed within a period of forty-five days from the date on which the person aggrieved receives a copy of the order made by the adjudicating officer

CYBER REGULATIONS APPELLATE TRIBUNAL (CRAT)

- As per the Act a provision has been made to appeal from the decision of the CRAT to the High Court within sixty days of the date of communication of the order or decision of the CRAT .

POWERS OF POLICE.

- A police officer not below the rank of Deputy Superintendent of Police, or any other officer authorized by the Central Government has the power to enter any public place and arrest any person without a warrant if he believes that a cyber crime has been or is about to be committed.

Network Service Providers

- Network services providers shall not be liable under this Act for any third party information or data made available, if they prove that the offence or contravention was committed without their knowledge or that they had exercised all due diligence to prevent such offence.
- Network service provider means an intermediary:
- Third party information means any information dealt with by network service provider in his capacity as intermediary

Offences by Companies

- In respect of offences by companies, in addition to the 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 the business of the company, shall be guilty of the contravention, unless he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.