

2012

INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008



CA AKHIL MITTAL

**BEFORE READING THIS
CHAPTER I WANT TO LET YOU
KNOW ALL THAT I AM NOT
EXPLAINING ALL PROVISIONS
OF THIS CHAPTER.....**

**SO PLEASE REFER MODULE IF
ANY ONE WANT TO COVER
ALL TOPICS....OTHERWISE
CAN CONTACT ME**

CHAPTER 10

INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

INTRODUCTION

In year 2000, both the houses of the parliament passed a **technology bill**. This bill is known as **INFORMATION TECHNOLOGY ACT, 2000**. It aimed at to provide legal framework under which LAEGAL SANCTITY is accorded to all the electronic transaction undertaken.

In year 2006, the act was amended & it passed in year 2008. And from now it is known as **INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008**.

IT ACT 2000 & ITS OBJECTIVES

This act provides **legal recognition** for transactions carried out by **means of electronic data interchange**. Objective of this act:

CODE TO REMEMBER: S.A.L.E.

A. Storage of data:

- ✚ Facilitate electronic storage of the data.

B. Amendment in other laws:

- ✚ This act results in simultaneous amendment following laws→
 - a. Indian Penal Code
 - b. The Indian Evidence Act, 1872
 - c. The Banker's book Evidence Act, 1891
 - d. Reserve Bank Of India, 1934

C. Legal recognition:

- ✚ To grant legal recognition:

BOA= Books of accounts

1. For transaction carried out by means of EDI.
2. To digital signatures for authentication.
3. For keeping banking BOA* in electronic form.

D. E-Filing Facilitation:

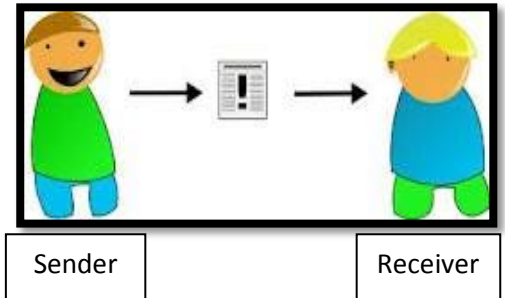
- ✦ Facilitate e-filing of documents with government departments.

DEFINITIONS1. ACCESS:

- ♣ Getting entry into logical, arithmetical or memory function resources of computer or computer network.

2. ADDRESSEE:

- ♣ Means a **person** who is intended by the **originator** to **receive the electronic records** not including any intermediary.

3. ADJUDICATING OFFICER:

- ♣ Means **officer** appointed under section 46(1).

4. AFFIXING ELECTRONIC SIGNATURE:

- ♣ Means **adoption of any methodology or procedure** by a person for the **purpose of authenticating ELECTRONIC RECORDS** by means of **electronic signature**.

5. APPROPRIATE GOVERNEMENT:

- ♣ Means:
 - e. Enumerated in **LIST II** of **seventh Schedule to constitution**.
 - f. Relating to any state law enacted under **LIST III** of **seventh Schedule to constitution**.

6. ASYMMETRIC CRYPTO SYSTEM:

- ♣ Means a **system of a secure key pair** consisting of a **PRIVATE KEY** for creating digital signature & a **public key** to verify the **digital signature**.

7. CERTIFYING AUTHORITY:

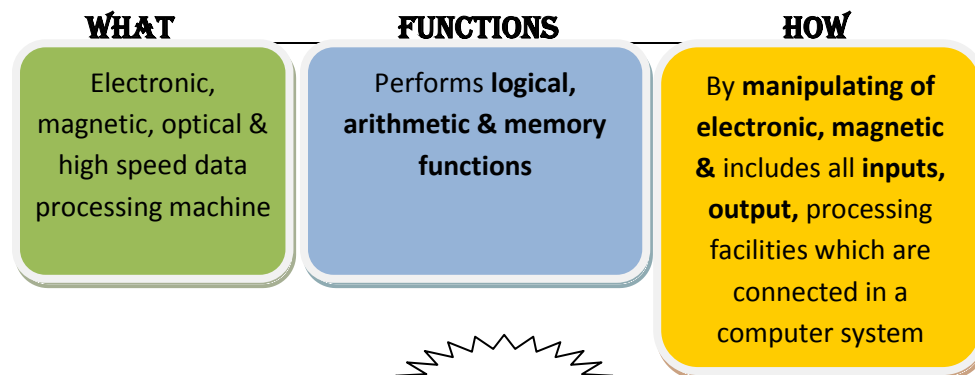
- ♣ Means a person who has been granted a **LICENSE** to issue a **ELECTRONIC SIGNATURE CERTIFICATE** under **SECTION 24**.

8. CERTIFICATE PRACTICE STATEMENT:

- ♣ Means a **statement issued by a CERTIFYING AUTHORITY** to specify the practices that certifying authority employs in issuing **electronic signature certificate**.

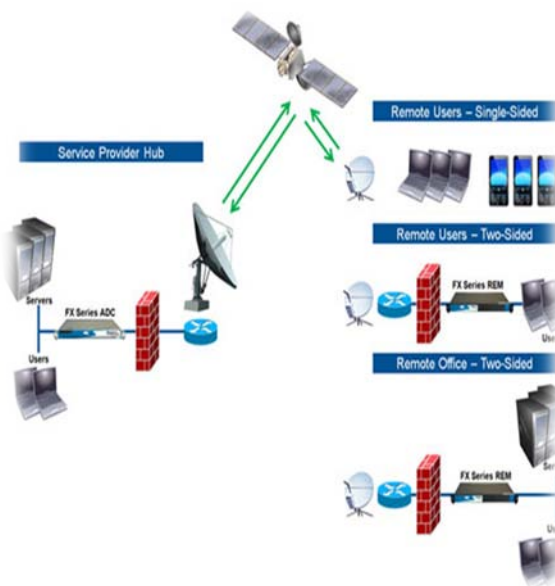
9. COMPUTER:

- ♣ Means



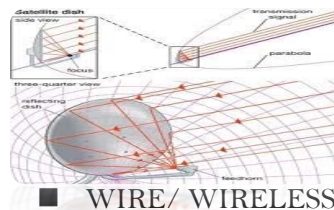
IT 2008

10. COMPUTER NETWORK



- ♣ Means **interaction of ONE or MORE computers/ computers system/ communication device** through:

■ USE OF SATELLITE



■ MICROWAVE



■ WIRE/ WIRELESS



■ WIRE AND WIRELESS

■ TERMINALS

11. COMPUTER RESOURCES: It includes the following:

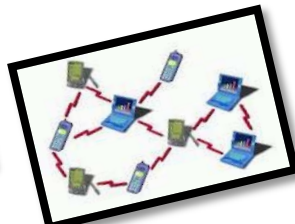
COMPUTER

COMMUNICATION DEVICE

COMPUTER SYSTEM

NETWORK

DATA



12. COMPUTER SYSTEM:

It means a **device** or a **collection of the devices**, including input & output devices capable for being used in conjunction with the external files containing computer programs, electronic instructions, input data, that **performs logic, arithmetic; data storage & retrieval**, communication control & other functions.

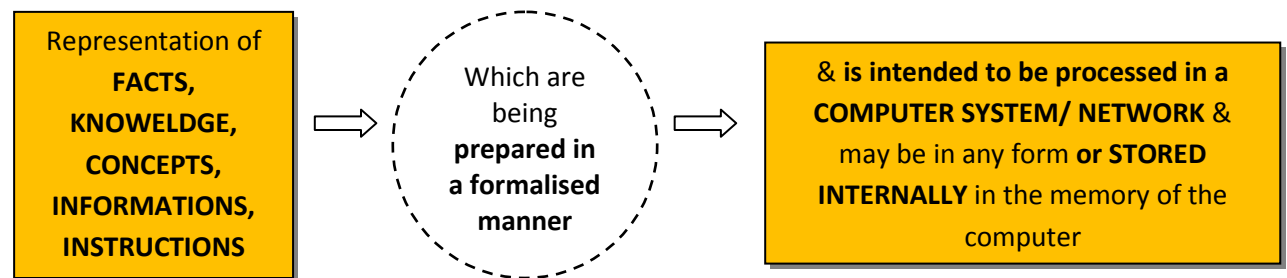
13. COMMUNICATION DEVICE:

Means: **Cell phone, personal Digital Assistance** or combination of both **used to COMMUNICATE, SEND OR TRANSMIT** text, audio, video or images.

IT 2008

14. CONTROLLER:

Means controller Of Certifying Authorities appointed under section 17(7).

15. DATA:**16. CYBER CAFÉ:**

IT 2008



Means **any facility from where access to internet** is offered by a person in ordinary course of business.

17. CYBER SECURITY:

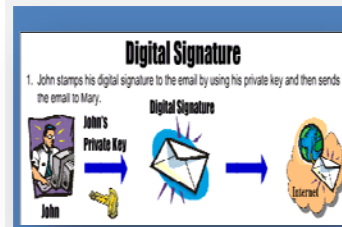
IT 2008



Means protecting information, equipment, devices, computer, computer resources, communication device,

& information stored therein from **UNAUTHORISED ACCESS, USE, DISCLOSURE** etc.

18. DIGITAL SIGNATURE :



Means

- Authentication of any electronic record by a subscriber,
- By means of an electronic method or procedure,
- In accordance with the section 3.

19. DIGITAL SIGNATURE CERTIFICATE:

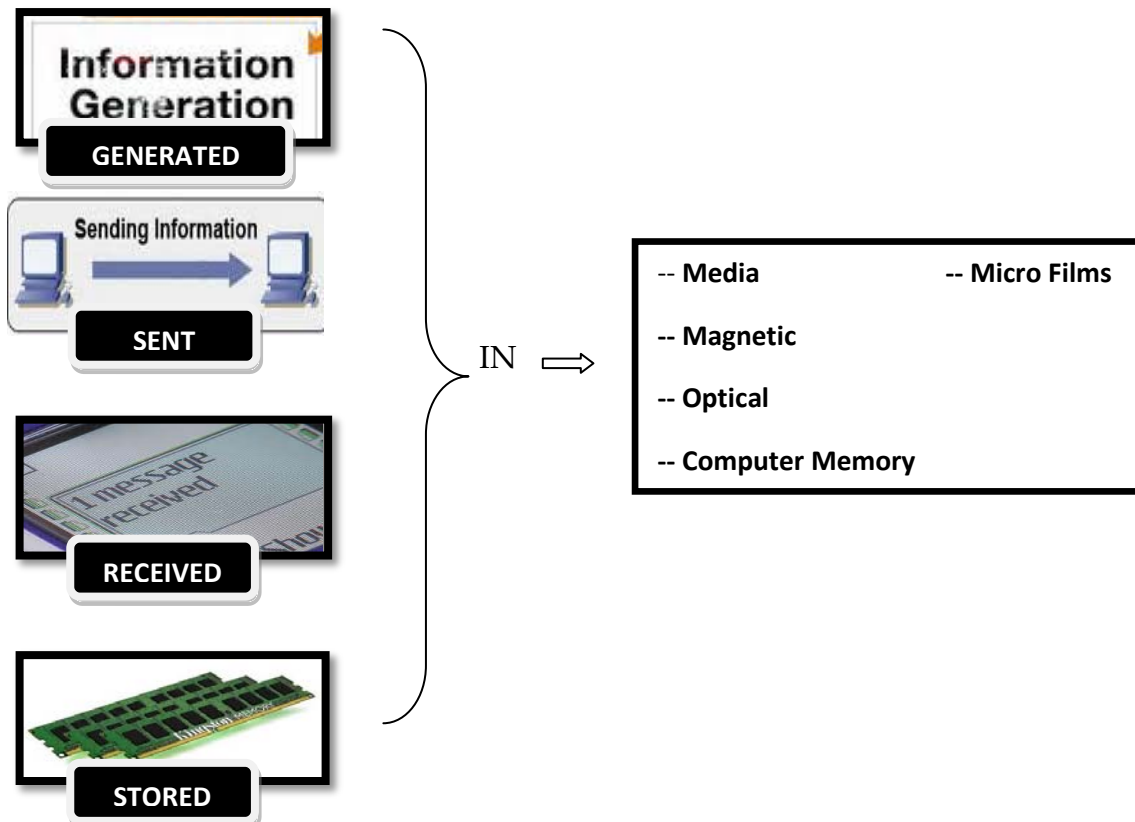


Means protecting information, equipment, devices, computer, computer resources, communication device,

& information stored therein from UNAUTHORISED ACCESS, USE, DISCLOSURE etc.

20. ELECTRONIC FORM :

With the reference to information means information



21. ELECTRONIC GAZETTE:

Means **OFFICIAL GAZETTE** published in the **ELECTRONIC FORM**.

22. ELECTRONIC RECORDS :

Means **DATA, RECORDS, IMAGES, SOUND (R.I.D.S.)** sent, received and stored in **an electronic form**.

23. ELECTRONIC SIGNATURE :

I am dividing the definition into 3 parts:

Authentication of any Records $\Rightarrow$ by a subscriber $\Rightarrow$ by means of electronic technique as in 2nd schedule & include digital signature

24. ELECTRONIC SIGNATURE CERTIFICATE:

Means an “**electronic signature certificate**” issued under **section 35** & includes **digital signature**

25. FUNCTION:

In relation to computer includes:

<u>L</u>-- Logical <u>C</u>--Control <u>C</u>--Communication <u>A</u>-- Arithmetic <u>R</u>--Retrieval <u>D</u>--Deletion <u>S</u>--Storage	}	<u>from or within computers</u>
--	---	---------------------------------

26. INFORMATION:

I am dividing the definition in following manner:

INFORMATION INCLUDES

IT 2008



-- DATA
-- MESSAGE
-- TEXT



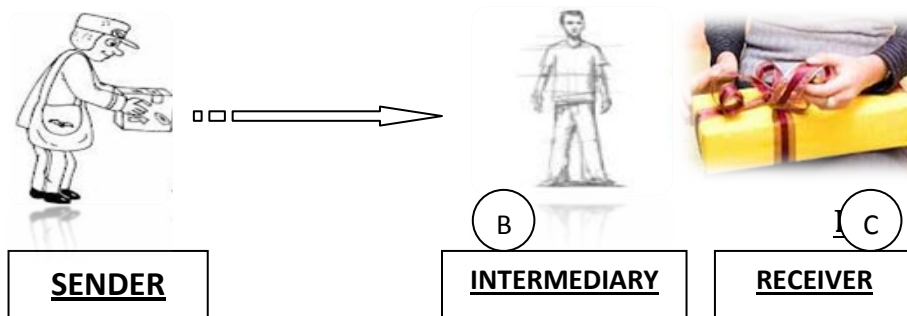
-- IMAGES
-- SOUND
-- VOICE



-- CODES
-- COMPUTER PROGRAM
-- SOFTWARE/ DATABASE

27. INTERMEDIARY:

Intermediary with respect to any particular **electronic records**, means



- ♣ Person **(B)** who on behalf of other **(C)** receives, stores or transmits **those records** with respect to that records etc.

28. KEY PAIR:

--It is **asymmetric crypto system**, means

--**PRIVATE KEY & ITS RELATED PUBLIC KEY** which are so related that public key can verify a **digital signature created by the private key**.

29. LICENSE:

It means license granted to certifying authority under section 24:

a. ORIGINATOR: **Person who**→

- ❖ send generates, stores or transmit any electronic,
- ❖ Or cause any electronic message to be sent, generated, stored,
- ❖ To any person

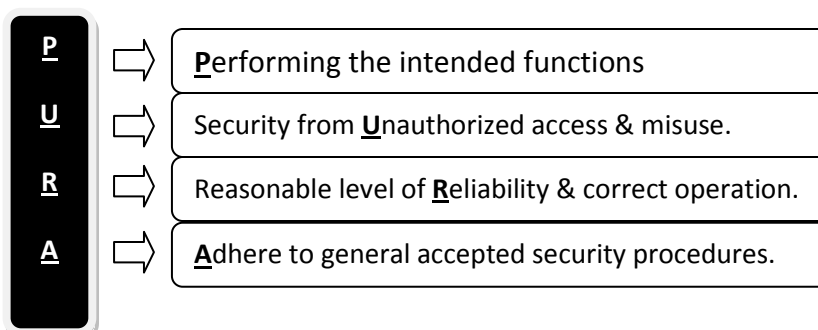
b. PRESCRIBED: Means prescribed by rules made under this act.

c. PRIVATE KEY: Key used to create a **DIGITAL SIGNATURE**.

d. PUBLIC KEY: Key used to **VERIFY** a **DIGITAL SIGNATURE** & listed in digital signature certificate.

30. SECURE SYSTEM:

Means **computer hardware, software & procedure** that:



31. SECURITY PROCEDURE :

Security procedure prescribed under section 16 by central government.

32. SUBSCRIBER:

Means a person in whose name the ELECTRONIC SIGNATURE CERTIFICATE is issued.

33. VERIFY:

In relation to a digital signature, electronic records or public key, to determine whether →

- e. Initial electronic records were affixed with the digital signature by use of private key corresponding to the public key of the subscriber.
- f. Initial electronic records are retained intact or have been altered since such electronic record was so affixed with the digital signature.

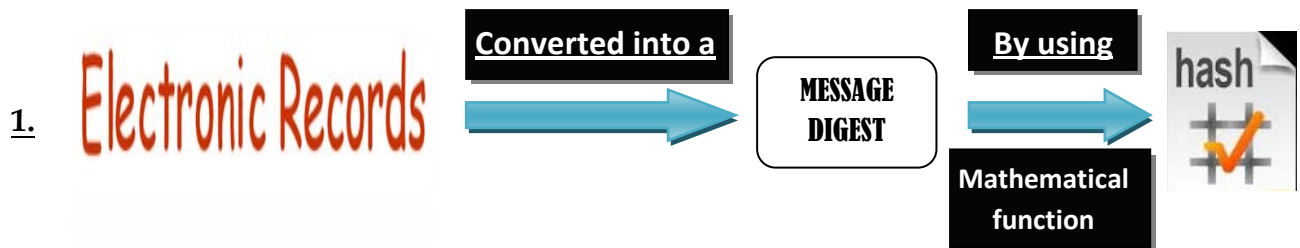
DIGITAL SIGNATURE & ELECTRONIC SIGNATURE

Chapter II

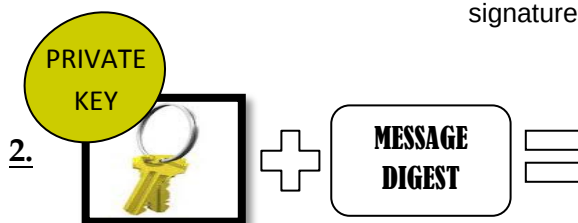
IT 2008

This chapter gives **LEGAL RECOGNITION** to electronics records & digital signatures. It contains only **SECTION 3**.

Digital signature is created in 2 distinct steps.



OUTCOME OF STEP 1: Hash function digitally freezes electronic records ensuring integrity of content of message. Any tampering with content will invalidate digital signature.



Identity of the person affixing the digital signature is **authenticated through the USE OF PRIVATE KEY** which can be verified by the receiver **by using public key** corresponding to that **private key**.

OUTCOME OF STEP 2: Private key being attached with the message digest helps anybody to verify whether electronic records are remained **INATCT**.

SECTION 3: AUTHENTICATION OF ELECTRONIC RECORDS

1. Subject to provisions of this section, **any subscriber may authenticate an ELECTRONIC RECORDS** affixing his **DIGITAL SIGNATURE**.
2. Authentication is effected by use of **ASSYMETRIC CRYPTOT SYSTEM & HASH FUNCTION** which transforms the electronic record in **another ELECTRONIC RECORD**.
3. **Any person by use of public key** of the subscriber **can verify ELECTRONIC RECORDS**.
4. **PRIVATE & PUBLIC** key are unique to **subscriber** & constitute a functioning key pair.

SECTION 3A: ELECTRONIC SIGNATURE

1. A subscriber may authenticate **any electronic records** by such electronic signature/ authentication technique which:
 - g. **Is considered reliable**
 - h. **May be specified in 2nd schedule**
2. Electronic signature/ authentication technique will be considered reliable If :
 - a) **Any alteration to information made after authentication is DETECTABLE.**
 - b) **Any alteration to electronic signature made after affixing is DETECTABLE.**
 - c) **Signature creation/authentication data are linked to AUTHENTICATOR & no other person**
 - d) **Signature creation/authentication data at time of SIGNING are under control of the AUTHENTICATOR & no other person**
 - e) **Other conditions as prescribed.**
3. Central government may prescribe the **procedure of ascertaining whether ELECTRONIC SIGNATURE is that of person by whom it is supposed to be AFFIXED.**
4. Central government (**Notification in OZ**) may **add or omit** any **electronic signature/ authentication.**
5. Such **notification in OZ** shall be **laid before EACH HOUSE OF PARLIAMENT.**

ELECTRONIC GOVERNANCE

Chapter III

It specifies the procedure to be followed for sending & receiving of electronic records & time & place of dispatch & receipt. This chapter contains SECTION 4-10.

SECTION 4: LEGAL RECOGNITION OF ELECTRONIC RECORDS

Where the law provides that **information is to be in written form, and then such requirement shall deemed to be satisfied** if such information is:

- ☐ **Made available in an ELECTRONIC FORM; AND**
- ☐ **ACCESSIBLE** so as to be **usable for a subsequent reference.**

SECTION 5: LEGAL RECOGNITION OF DIGITAL SIGNATURE

Where the law provides that **information** should be **authenticated by affixing the signature** of any person **then such requirement shall deemed to be satisfied** if:

- ☐ **It is authenticated by means of DIGITAL SIGNATURE** affixed in such way as **CG prescribed.**

SECTION 6: USE OF ELECTRONIC RECORDS & SIGNATURE IN GOVERNMENT & ITS AGENCIES

Where any law provides for:

- ☐ Filing of any form, application etc **with office, authority, government agencies** in particular manner
- ☐ Issue/grant of **any license, sanction, approvals** in a particular manner.
- ☐ Receipt/payment of money in a particular manner.



Such requirement shall be deemed to be satisfied if such Filing of any form, Issue/grant of **any license, receipt/payment of money is affected by means of electronic form.**

SECTION 6A: DELIEVER OF SERVICES BY SERVICE PROVIDER

IT 2008

CODE TO REMEMBER: S.A.M.

1. SCALE OF SERVICE CHARGES:

- ✱ Appropriate government, **notification in OZ**, specifies the **scale of service charges** which may be charged by the service provider under this section.

2. AUTHORISATION BY APPROPRIATE GOVERNMENT:

- ✕ Appropriate government may authorize **any service provider** to:
 - f) **Collect, retain & appropriate service charges for the purpose of providing services from the person availing such services.**
 - g) **Collect, retain & appropriate e-charges by the service provider.**

3. MAINTEIN & UPGRADE FACILITIES:

- ✕ Appropriate government may authorize by order, **to MAINTAIN & UPGRADE** the **COMPUTERIZED FACILITIES & perform such functions as specify in the official gazette.**

SECTION 7: RETENTION OF ELECTRONIC RECORDS

Where law provides that **documents, records etc** to be retained for specific period, then such requirement shall **be deemed to be satisfied** if such records are in **ELECTRONIC FROM:**

- (A) **Information contained remains accessible so as to be usable for subsequent reference.**
- (B) **Electronic records are maintained in the FROMAT IT IS ORIGINAL GENERATED, sent or received.**
- (C) **The details which will FACILIATTE the identification of the origin, destination, date & time of dispatch of such electronic records are available in ELECTRONIC RECORD.**

SECTION 7A: AUDIT OF DOCUMENTS ETC IN ELECTRONIC FORM

Where law provides, there is **provision for AUDIT OF DOCUMENTS, RECORDS & INFORMATION**, then same rule will applicable in respect of **ELECTRONIC FROMS.**

SECTION 8: PUBLICATION OF RULES, REGULATIONS ETC IN ELECTRONIC GAZETTE

Where law provides, that any **rules, regulations, order, bye laws** have to published in **Official Gazette**, then such requirement deemed to be **satisfied** if **such rules, regulations, order, bye laws** published in the **ELECTRONIC GAZETTE.**

SECTION 10: POWER TO MAKE RULES BY CENTRAL GOVERNMENT IN RESPECT OF ELECTRONIC SIGNATURE



Central government may prescribe:

CODE TO REMEMBER: M.-C.P.T.

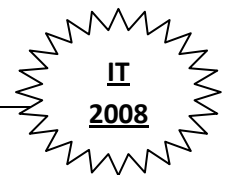
- A. Manner & format in which electronic signature shall be affixed.
- B. Control processes / procedures to ensure **adequate integrity, security & confidentiality of electronic records/payments.**
- C. Procedure which facilitate **identification** of person **affixing electronic signature**
- D. Type of Electronic Signature.

ATTRIBUTES, ACKNOWLEDGMENT & DISPATCH OF ELECTRONIC RECORDS

Chapter IV

This chapter deals with **attribution, receipt & dispatch of electronic records**. This mainly deals with the way how **an electronic record** is to be **attributed** to person who originated it.

SECTION 11: ATTRIBUTION OF ELECTRONICS RECORDS



An electronic record shall be attributed to the originator:

- ☯ If it was sent by the **originator himself**. [khud bheja maine]
- ☯ By a person who had **authority to act** on behalf of originator in respect of electronic records.
[Mere behalf par Kisi aur ne bheja]
- ☯ By an **information system programmed by** on behalf of originator to operate automatically.
[Mere behalf par system programmer ne bhej di automatically]

I am not explaining the Section 12 & 13.....This is not important ...So I am leaving it

SECURE ELECTRONIC RECORDS & SECURE ELECTRONIC SIGNATURE

This chapter sets out **THE CONDITION** that would apply to **QUALIFY ELECTRONIC RECORDS & DIGITAL SIGNATURE** as being secure. **It contains SECTION 14 TO 16.**

SECTION 14: SECURE ELECTRONIC RECORDS**-- What is secured Electronic Records?**

"Where any security procedure is applied to an electric record **at a specific point of time**, then such records shall deemed to be secure electronic record from such point of time to time of verification."

SECTION 15: SECURE ELECTRONIC SIGNATURE

An electronic signature shall be deemed to be secured if:

- h) Signature creation data, at **time of fixing** signature was under the exclusive control of **signatory** & no other person.
- i) **Signature creation data** was stored in such manner as prescribed.

SECTION 16: SECURE PROCEDURES & PRACTICES

Central government may prescribe the security procedures & practices. It may take into consideration the **commercial circumstances, nature of transaction & other related factors.**

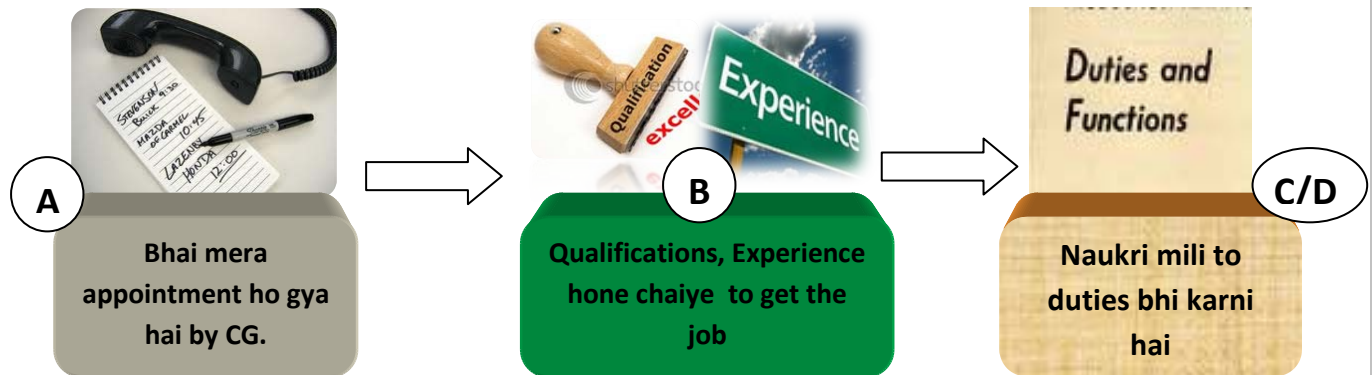
REGU LATION OF THE CERTIFYING AUTHORITIES

This chapter contains DETAILED PROVISIONS relating to the appointment & powers of the CONTROLLER & CERTIFYING AUTHORITIES. It contains section 17 to 34.

SECTION 17: APPOINTMENT OF CONTROLLER & OTHER OFFICERS

IT
2008

I am dividing the points in such a manner that they can be understood with ease.



IT
2008

A. Central government, **by notification in official gazette**, appoints a **Controller Of certifying Authorities, Deputy Controller & assistant controller**, other officers & employees.

IT
2008

B. Qualification, Experience & terms and conditions of services of **Controller Of certifying Authorities, Deputy Controller & assistant controller**, other officers & employees, As prescribed by the **central government**.

C. The **Controller** shall discharge function subject to **general control & directions** of central government.

D. The **Deputy Controller & Assistant Controller** shall discharge function subject to **general superintendence & control** of the controller.

E. **HEAD AND BRANCH OFFICE** of the controller shall be a such places as the central government may specify.

F. There shall be **seal** of **the office of the controller**.

SECTION 18: FUNCTIONS OF CONTROLLER

CODE TO REMEMBER: Q.C. --- D.S.S. --- R.E.M.

Quality **C**ontrol on **DSS** (Decision Support System) & **REM** - Ye function h mera

A. Qualification specifying:

- ✧ Specifying qualifications and experience which employees of **certifying authority** possess.

B. Certification public key:

- ✧ Certifying public keys of the certifying authorities.

C. Duties specification:

- ✧ Laying down the duties of the **certifying authority**.

D. Supervision:

- ✧ Exercising supervision over the activities of the certifying authorities.

E. Standards fixation:

- ✧ Laying down the standards to be maintained by the CERTIFYING AUTHORITIES.

F. Resolving conflicts:

- ✧ Resolving **any conflict of INTEREST** between certifying authorities & subscribers.

G. Establishing electronic system:

- ✧ Facilitating the **establishment of electronic system** by a certifying authority **either solely or jointly** with the certifying authority.

H. Maintaining Database:

- ✧ Maintaining the DATABASE containing the disclosure records of every certifying authority which shall be accessible to public.

SECTION 21: LICENSE TO ISSUE ELECTRONIC SIGNATURE CERTIFICATES



- (1) Subject to provisions of **sub section (2)**, applicant may make application to Controller for a license to issue electronic signature certificate.
- (2) No license shall be issued under **sub section (1)**, unless applicant doesn't fulfill all **requirements**, which are necessary to issue electronic signature certificates.

(3) A license granted under this section shall:

- j) Be valid for the period specified by the central government.
- k) Not be transferable or heritable
- l) Be subject to terms & conditions as specified by the regulations.

SECTION 22: APPLICATION FOR LICENSE

(1) Every application for issue of a **license** shall be in such a form as prescribed by the **central government**.

(2) Every application shall be accompanied with:

- m) **Certification Practice Statement**
- n) **Statement including PROCEDURES with respect to applicant identification.**
- o) **Payment of FEES ≤ 25,000** as prescribed by the **central government**.

SECTION 23: RENEWAL OF LICENSE

(1) An application for renewal of a license shall be:

- p) **In such a form,**
- q) **Accompanied by fees ≤ 5,000 as prescribed by CENTRAL GOVERNMENT** shall be made not less than **45 days** before the expiry of period of validity of the license.

SECTION 24: PROCEDURE FOR GRANT OR REJECTION OF LICENSE

The controller may, ON RECEIPT OF APPLICATION under **section 21(1)**, after considering **DOCUMENTS** accompanying the **application**, may **GRANT OR REJECT** the application.





SECTION 25: SUSPENSION OF LICENSE (F - T.C.S)

The controller may cancel the license if it thinks that **certifying authority**:

- r) Made a statement in respect of application for **issue/renewal** which is **INCORRECT/FALSE. (F)**
- s) **Failed to comply with TERMS & CONDITIONS. (T)**
- t) **Failed to maintain the SATNDARDS (S)**
- u) **CONTRAVENED** any provisions of this act **(C)**.

However, no revocation unless **certifying authority** is given reasonable opportunity of being heard.



SECTION 26: NOTICE OF SUSPENSION/REVOCATION OF LICENSE

Where the license of the **Certifying Authority** is suspended or revoked, the **CONTROLLER** shall publish **NOTICE OF SUCH SUSPENSION** in the **DATABASE** maintained by him.

SECTION 27: POWER TO DELEGATE

The **CONTROLLER** in writing may, authorize the **DEPUTY & ASSISTANT CONTROLLER** to exercise any power of the **powers of the controller under this chapter.**



SECTION 28: POWER TO INVESTIGATE INTERVENTION

- (1)** The **controller or person authorized** by him shall take up for **investigation** any contravention of the provisions of the act.
- (2)** The person authorized by the **CONTROLLER** shall exercise **POWERS** which are conferred on **INCOME TAX AUTHORITIES** under **CHAPTER XIII** of income tax act 1961.

SECTION 29: ACCESS TO COMPUTERS AND DATA

(1) The **CONTROLLER/ person authorized by him**, if he has reasonable cause to suspect **access to data, computer system**, for the purpose of **searching to obtain INFORMATION** contained in such system.

(2) The **CONTROLLER/ person authorized by him**, by order direct any person to **PROVIDE HIM assistance**.



SECTION 30: DUTIES OF CERTIFYING AUTHORITY

CODE TO REMEMBER: S.O.A.R.

This section provides that **CERTIFYING AUTHORITY** shall follow certain procedures in respect of **DIGITAL SIGNATURE**:

i. **Secured facilities:**

- ☉ Make use of **secured hardware, software & procedures** free from unwanted **intrusion & misuse**.

ii. **Observe other standards as specified by the regulations.**

iii. **Adherence to security procedures:**

- ☉ Adherence to security procedures to **ENSURE** that secrecy & privacy of **electronic signature ARE ASSURED**.



iv. **Reasonable reliability:**

- ☉ Made a **reasonable level of REALIBILITY** in its **SERVICES** which are best suited to **performance of intended functions**.

SECTION 31: CERTIFYING AUTHORITY TO ENSURE COMPLIANCE OF ACT

Every certifying authority shall ensure that **every person employed** engaged by it, in the **course of his employment COMPLIES** with rules, regulations & orders made there under.

You are about to Surrender your License. Continue ?

Yes or No

SECTION 32: DISPLAY OF LICENSE

Every **certifying authority** must display its **LICENSE** at a place from where it carries on its business.



SECTION 33: SURRENDER OF LICENSE

-- Certifying authority whose **LICENSE** is revoked/suspended —→ shall **surrender license to Controller**

-- Where the **certifying authority** fails to surrender the license:

☐ **IMPRISONMENT:** Extended up to 6 years

OR

☐ **FINE** : Extend up to 10,000

OR

BOTH

SECTION 34: DISCLOSURE



(1) Every certifying authority shall disclose in manner specified by regulations:

✚ Its **ELECTRONIC SIGNATURE CERTIFICATE**

✚ **CERTIFICATE PRACTISE CERTIFICATE**

✚ **NOTICE OF REVOCATION/SUSPENSION**

✚ **FACTS** affecting the reliability of **electronic signature certificate**.

IT 2008

(2) Where certifying authority **is of opinion that** any situation **may adversely affect the INTEGRITY OF ITS COMPUTER SYSTEM**, then certifying authority shall:

✚ Use reasonable efforts to notify any person who is likely to be affected by that occurrence.

✚ Act in accordance with the procedure specified in its **CERTIFICATION PRACTICE STATEMENT**.

Chapter VII

ELECTRONIC SIGNATURE CERTIFICATES

*This chapter contains DETAILED PROVISIONS relating to **DIGITAL SIGNATURE CERTIFICATE**. The application shall be accompanied by a fee not exceeding **Rs. 25,000**. Contains section 35 to 40.*

*This section also provides that **no digital signature certificate** shall be granted unless the **certifying authority is satisfied** that:*

- (a) The applicant the **private key** corresponding to **public key** to be listed in **digital signature certificate**.
- (b) Applicant holds **private keys** capable of **creating digital signature**.
- (c) Public key to be listed in the **certificate** can be used to verify a **digital signature certificate** affixed by the private key.

*No application to be rejected unless the **applicant** is given the opportunity of **being heard**.*

SECTION 36: REPRESENTATION UPON ISSUANCE OF DIGITAL SIGNATURE CERTIFICATE



A certifying Authority while issuing a **digital signature certificate** shall certify that:

- a) It has **complied with provisions of this act, rules & regulations**.
- b) It has **published the DIGITAL SIGNATURE** certificate or **made available to person relying on it & subscriber has accepted it**.
- c) The **subscriber** holds the **private key** corresponding to **public key**, listed in digital signature certificate :
 - ☐ **Subscriber holds a private key capable of creating digital signature.**
 - ☐ **Public key can be used to verify a digital signature affixed by private Key held by the subscriber.**
- d) The **subscriber's** public key & **private key** constitute a **functioning KEY PAIR**.
- e) Information contained in **digital Signature Certificate** is **ACCURATE**.
- f) Has no knowledge of the material facts **that can adversely affect the reliability** of representation.



CHAPTER VII DEALS WITH THE WORKING OF THE CERTIFYING AUTHORITY. WE WILL DISCUSS HERE THE PROCEDURE OF ISSUE/SUSPENSION/REVOCATION OF DIGITAL SIGNATURE CERTIFICATE ISSUED BY THE CERTIFYING AUTHORITY TO THE SUBSCRIBER

SECTION 37: SUSPENSION OF DIGITAL SIGNATURE CERTIFICATE

Reason for suspension: If certifying authority is of opinion that steps need to be taken **in public interest**.

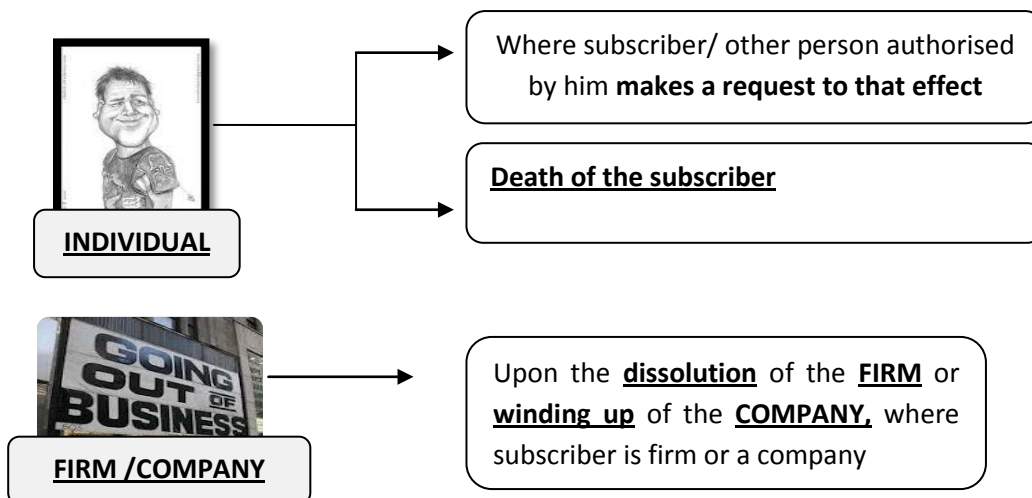
Such certificate shall not be suspended for a period exceeding 15 DAYS unless the subscriber has been given OPPORTUNITY OF BEIGN HEARD.

Certifying authority may suspend the digital signature certificate if:

- ☐ Receipt of request from the **SUSBSCRIBER** listed in **digital signature certificate**. [khud request]
- ☐ Receipt of request from person authorized to act on behalf of that subscriber. [kisi aur ne request ki jo subscriber ke behalf par doing work]

SECTION 38: REVOCATION OF DIGITAL SIGNATURE CERTIFICATE

A certifying Authority may revoke **digital signature certificate** issue by it:



Certifying authority may also revoke a **digital signature certificate**, if it is of opinion that:

- ✘ A material fact represented in **DIGITAL SIGNATURE** is **FALSE OR CONCEALED**.
- ✘ Requirement for **issuance** of digital signature **WAS NOT SATISFIED**.

DUTIES OF SUBSCRIBERS

This chapter contains **section 40 to 42**. It specifies **DUTIES OF THE SUBSCRIBERS**. As per **ITAA 2008**, different sections are as follow:

SECTION 40: GENERATING KEY PAIR

Where digital signature is accepted by the subscriber, then he shall generate that **KEY PAIR** by applying the security procedure.

SECTION 41: ACCEPTANCE OF DIGITAL SIGNATURE CERTIFICATE

A subscriber shall be deemed to have accepted a **DIGITAL SIGNATURE CERTIFICATE**, if he publishes or authorize the publication of a **digital signature certificate**-

- ☐ To one or more persons,
- ☐ In a **REPOSITORY**, or demonstrate his **APPROVAL** in any manner.

Accept karne ke different ways

By accepting Digital signature certificate, **subscriber verifies that**:

Accept karne ke baad kya hga?

- ☐ Subscriber holds the **private key** corresponding to public key listed in **digital signature certificate & is entitled to hold the same**.
- ☐ All representation made by subscriber to the certifying authority are **TRUE**.
- ☐ All information contained in **digital signature certificate** is within **KNOWLEDGE** of subscriber is **TRUE**.

PENALTIES & ADJUDICATION

This chapter contains **section 43 to 47**. It provides for **awarding compensation/damages** for certain type of **computer frauds**.

It also provides **appointment of adjudication officer** for holding an inquiry in **relation to certain computer crimes & for awarding compensations**.

SECTION 43: PENALTIES & COMPENSATION FOR DAMAGE TO COMPUTERS, COMPUTER SYSTEM, ETC



CODE TO REMEMBER: A.M.C. - D.V.D.

AMC (Annual Maintenance Cost) of DVD

If any person **without permission** of the owner / any other person who is in-charge of computer, computer resources--

1. Access to computers:

✚ Accesses or **secure access** to such computer, computer resources, computer network.

IT 2008

2. Manipulation of information:

✚ Destroys, deletes or **alters** any **information** in the computer resources, or use it in such a manner that it **diminishes/reduces** the value of the information.

IT 2008

3. Concealment of computer resource:

✚ Steals, conceals, destroy / or cause any person to steals, conceals, destroy **any computer source code** with an intention to cause damage.

IT 2008

4. Download of information:

✚ Downloads copies or extracts any **data, database** from such computer, computer resources or computer network.

5. Virus in computer system:

✚ Introduces, or cause to introduce **any computer virus/any computer contaminant** into any computer system or computer network.

6. Disruption in computer network:

✚ Disrupts or cause **disruption** of any **computer, computer system or computer network**.

1. COMPUTER CONTAMINANT:

It means set of computer instructions that are designed:

- To modify, destroy, record data/program in computer OR
- By any mean to usurp (seize or hold) normal operations of computer.



2. DAMAGE:

Means destroy, alter, delete, add, and modify **[MADAD]** re-arrange any computer resources.



3. COMPUTER DATABASE:

It means representation of:

- Information, knowledge, facts, concepts in [I, KFC]
- Image, video, audio, text [I,VAT]
- That are being **prepared in formalised manner** or have been produced,
- By computer, computer resources, computer network.

**4. COMPUTER VIRUS:**

It means:

- Computer instruction, information, data or program
- **That destroy, damage, degrades & adversely affect performance of computer or**
- Which attach itself with other computer resources & operates when a program is executed.



SECTION 44: PENALTY FOR FAILURE TO FURNISH INFORMATION, RETURN ETC



Any person who is required under this act:

REASON OF PENALTY IMPOSITION	AMOUNT OF PENALTY
<u>F</u>urnish any documents, return or report to the controller or certifying authority, FAILS to furnish the information,	Not exceeding Rs. 1,50,000.00 ≤ 1,50,000.00 [for each failure]
<u>R</u>eturn / information not furnished within the time as specified in the regulations	Not exceeding Rs. 50,000.00 ≤ 50,000.00 [for every day during which such failure continues]
<u>B</u>ook of accounts are not maintained	Not exceeding Rs. 10,000.00 ≤ 10,000.00 [For every day during which such failure continues]

SECTION 45: RESIDUAL PENALTY

REASON OF PENALTY IMPOSITION	AMOUNT OF PENALTY
For which no penalty is separately provided separately	Not exceeding Rs. 25,000.00 ≤ 25,000.00

SECTION 46: POWER TO ADJUDICATE

For adjudging under this chapter, central government shall appoint any officer NOT BELOW THE RANK OF A DIRECTOR to the government of India,

OR

Any equivalent officer of a state government to be an **adjudicating officer** for holding **inquiry** in the manner prescribed by the central government

IT 2008

LEVEL OF OFFICER	LIMIT OF AMOUNT
<u>Adjudicating Officer</u> appointed above shall adjudicate matters in which	<u>CLAIMS</u> for injury or damage doesn't exceed <u>5 crore</u> ≤ 5,00,00,000.00
<u>Competent Court</u>	<u>CLAIMS</u> for injury or damage exceed <u>5 crore</u> ≥ 5,00,00,000.00

IT 2008

OFFICER APPOINTMENT	QUALIFICATION
Appointment of adjudicating Officer	He must possess experience in field of: <u>Information Technology</u> <u>Legal or judicial Experience</u>

Adjudicating officer must give opportunity to person who is guilty of **contravention**, reasonable opportunity of being heard to be given.

SECTION 47: FACTORS TO BE TAKEN INTO ACCOUNT BY THE ADJUDICATING OFFICER

While **adjudicating the QUANTUM of COMPENSATION**, the adjudicating officer shall consider the following factors:

- i. The **amount of GAIN of unfair ADVANTAGE** made as result of default.
- j. The amount of **LOSS** caused to any person as result of default.
- k. The **repetitive nature** of the default

THE CYBER APPELLATE TRIBUNAL



Chapter X

SECTION 48: ESTABLISHMENT OF CYBER APPELLATE TRIBUNAL



Central government -----> By notification, establish 1 or more appellate tribunals
to be known as *CYBER APPELLATE TRIBUNAL*.

SECTION 49: COMPOSITION OF CYBER APPELLATE TRIBUNAL

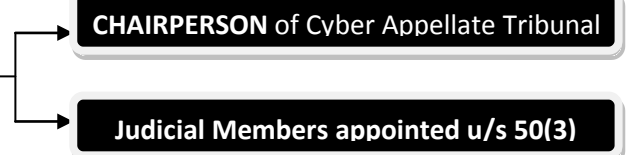
1. Composition = chairperson + other members [as the central government, by notification in official gazette, appoints]
2. Selection by CENTRAL GOVERNMENT in consultation with CHIEF JUSTICE OF INDIA.



3. Subject to provisions of this act:

- a. Jurisdiction, powers & authority of **cyber appellate Tribunal** may be exercised by **benches**.
- b. **BENCH** = Chairperson + 1/2 members as chairman may deem fits.

Provided that every bench shall
Be presided over by the



- c. Benches of **Cyber Appellate Tribunal** shall sit at NEW DELHI.
- d. Central government may specify the area of jurisdiction of each bench, by notification in **OFFICIAL GAZETTE**.

IT 2008

4.



IT 2008

The **CHAIRPERSON** of the **cyber Appellate Tribunal** may transfer a **member** of such tribunal from **ONE BENCH** to **ANOTHER BRANCH**.

5. If chairman thinks at any stage of hearing of a matter, that matter requires **more members**, then such **case** or **matter** may transferred to such larger bench.

SECTION 50: QUALIFICATIONS FOR APPOINTMENT AS CHAIRPERSON & MEMBERS OF CYBER APPELLATE TRIBUNAL



1.

PERSON WHO IS QUALIFIED TO BE

IT 2008

HE IS

HAS BEEN

QUALIFIED TO BE



JUDGE OF HIGH COURT

2.

MEMBERS OF CYBER APPELLATE TRIBUNAL

WHO WILL APPOINT**CENTRAL GOVT.**KNOWLEDGE REQUIRED

Having **specialised knowledge in INFORMATION TECHNOLOGY, INDUSTRY, TELECOMMUNICATION, MANAGEMENT & CONSUMER AFFAIRS**

PERSON SHALL BE APPOINTED AS MEMBER, IF

IT 2008

HE IS

HAS BEEN

Held post of **Additional secretary to Govt. Of India / equivalent post on CG /SG**

≥ 2 years

Held post of **joint secretary to Govt. Of India / equivalent post on CG /SG**

≥ 7 years

3.WHO WILL APPOINTKNOWLEDGE REQUIRED

**JUDICIAL MEMBER OF
CYBER APPELLATE
TRIBUNAL**

IT 2008

CENTRAL GOVT.

Has been member of **INDIAN LEGAL SERVICES**, & held the position of **additional secretary** for a **PERIOD OF less than 1 YEAR**

SECTION 51: TERMS OF OFFICE, CONDITIONS OF SERVICES ETC OF CHAIRPERSON & MEMBERS



I am presenting the provisions in tabular format:

IT 2008

CHAIRPERSON/ MEMBER	TENURE
The chairperson/members of cyber appellate tribunal shall held office	For a term of 5 YEARS
	
	From date on which he enter upon his OFFICE OR Until he ATTAINS age of 65 years
	WHICHEVER IS ERLIER

SECTION 52: SALARY, ALLOWANCE & OTHER TERMS & CONDITIONS OF SERVICES ETC OF CHAIRPERSON & MEMBERS

SALARY & ALLOWANCE = PENSION + GRATUITY + RETIREMENT BENEFIT



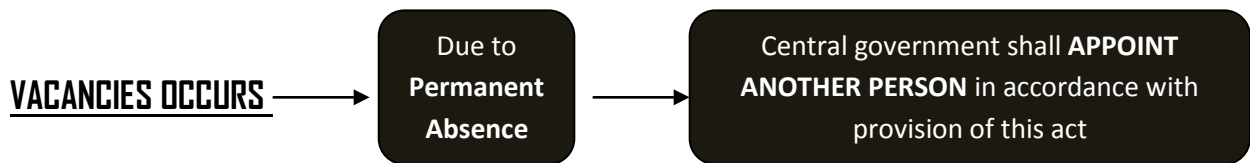
IT 2008

SECTION 52C: POWERS OF CHAIRPERSON TO TRANSFER CASE



SECTION 53: FILLING OF VACANCIES

IT 2008



SECTION 54: RESIGNATION AND REMOVAL

IT 2008



SECTION 54: APPEAL TO HIGH COURT

WHO CAN APPEAL

REASON FOR APPEAL

TIME LIMIT



Chapter XI

OFFENCES

This chapter contains **sections 65 to 78**. It deals with **computer crimes & provides penalties for these offences**.

I am hereby representing the topics in **TABULAR FORMAT**:

SECTION NUMBER	KIND OF OFFENCE	PENALTIES OF OFFENCES
CODE TO REMEMBER : CD-SR [CD of SIR]		
65	Intentionally <u>C</u> oncealment, destroy, alteration any source code , computer program , computer system , network , resources etc	IMPRISONMENT 3 YEARS OR FINE 2,00,000.00 OR BOTH

66 IT 2008	<u>D</u> amage to computer, computer resources, by doing acts defined in section 43	<u>IMPRISONMENT</u> 3 YEARS OR <u>OR BOTH</u>	<u>FINE</u> 5,00,000.00
66A IT 2008	<u>S</u> ending offensive messages through communication services etc --Info. Having threat character --Info which is false & is being communicated to cause danger -- Email send to deceive to mislead the recipient about message origin point	<u>IMPRISONMENT</u> 3 YEARS and	<u>FINE</u>
66B IT 2008	<u>R</u> eceiving dishonestly any stolen computer resources or communication devices	<u>IMPRISONMENT</u> 3 YEARS OR <u>OR BOTH</u>	<u>FINE</u> 1,00,000.00
CODE TO REMEMBER : I. -C.V.C.			
66C IT 2008	<u>I</u> dentification theft_fraudulently by making use of the ELECTRONIC SIGNATURE, PASSWORD	<u>IMPRISONMENT</u> 3 YEARS AND	<u>FINE</u> 1,00,000.00
66D IT 2008	<u>C</u> heating by personation by using computer resources.	<u>IMPRISONMENT</u> 3 YEARS AND	<u>FINE</u> 1,00,000.00
66E IT 2008	<u>V</u> iolation of the privacy of any person	<u>IMPRISONMENT</u> 3 YEARS OR <u>OR BOTH</u>	<u>FINE</u> 2,00,000.00
66F IT 2008	<u>C</u> yber Terrorism done with: --Intent to threaten integrity of India --Intentionally penetrates a computer resources result in damage to property	<u>IMPRISONMENT</u> LIFETIME	
67 IT 2008	<u>P</u> unishment for publishing or transmitting OBSCENE MATERIAL in electronic form	<u>CONVICTION</u> 1 st Subsequent	<u>IMPRISONMENT</u> 3 YEARS & 3 YEARS <u>FINE</u> 5,00,000.00 & 10,00,000.00

67A	<u>P</u>unishment for publishing or transmitting of MATERIAL contain sexually explicit act etc in electronic form	<u>CONVICTION</u> 1 st Subsequent	<u>IMPRISONMENT</u> 5 YEARS 7 YEARS	<u>FINE</u> & 5,00,000.00 & 10,00,000.00
67B	<u>P</u>unishment for publishing or transmitting of MATERIAL depicting children in sexually explicit act etc in electronic form	<u>CONVICTION</u> 1 st Subsequent	<u>IMPRISONMENT</u> 5 YEARS 7 YEARS	<u>FINE</u> & 5,00,000.00 & 10,00,000.00

@@@@@@@@ I AM HEREBY ENDING THIS CHAPTER@@@@@@@@