STUDY MATs

SEC 3.1 Chg

Information Technology & Its Application in Business (Theory -50 + Practical- 50)

Unit1: Information Technology and Business [8 Marks, Class: 8]

Data are facts, set of symbols to represent objects, events, activities and quantities. The word 'data' is the plural of the word 'datum', which means fact. Therefore, data means any collection of facts. Data can be considered as the raw material of information. The data may be numerical such as sales report, inventory figures etc. or non-numerical like customer's names, addresses etc. Data can be classified as:

Fact – e.g., price of a printer.

Event – e.g., arrival of new stock or a patient has reported to the doctor's receptionist. Transaction – e.g., making a booking.

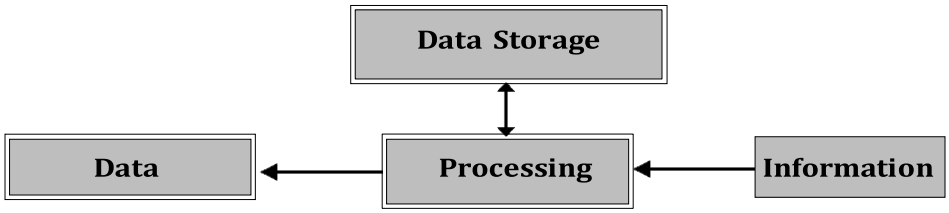
A hierarchy of several levels of data has been devised that differentiates between different groupings or elements, of data. Data are logically organized into the following manners:

1. ***Character:*** It is the most basic logical data element. It consists of a single alphabetic, numeric, or other symbol.
2. ***Field:*** It consists of a grouping of The related fields of data are grouped to form a record. Thus, a record represents a collection of attributes that describe an entity. Fixed-length records contain, a fixed number of fixed-length data fields. Variable-length records contain a variable number of fields and field lengths.
3. ***File:*** A group of related records is known as a data file or table. Files are frequently classified by the application for which they are primarily used, such as a payroll file or an inventory file, or the type of data they contain, such as a document file or a graphical image file. Files arealso classified by their permanence, for example, a master file versus a transaction file. A transaction file would contain records of all transactions occurring during a period, whereas a master file contains all the permanent records. A history file is an obsolete transaction or master file retained for backup purposes or for long-term historical storage called archival storage.
4. ***Database:*** It is an integrated collection of logically related records or objects. A database consolidates records previously stored in separate files into a common pool of data records that provides data for many applications. The data stored in a

database is independent of the application programs using it and of the ‘type of secondary storage devices on which it is stored.

CONCEPT OF INFORMATION

Data arranged in certain order and form which is useful to the recipient is called Information. ***Davis & Olson*** define a fairly good definition as, “data that have been processed into a form that is meaningful to the recipient and is of real or perceived value in current or prospective actions



Features of Information

The information has some features or attributes that give more value to informationprocessing system and make it more useful. The most important features are following:

(i) Information adds to a representation.
It corrects or confirms previous information

(ii) Information adds to a representation.

(iii) It corrects or confirms previous information.

(iv) It has surprise element or news value.

(v) It reduces uncertainty.

(vi) It has value in decision-making.

(vii) It is reusable.

Good Quality of Information

A good quality of information should be:

(i) ***Brief –*** Vital facts in summary form without lots of extraneous detail. Exception reports list items on which there needs to be action.

(ii) ***Accurate –*** Inaccurate data leads to poor decisions. Some decisions may be based on probability.

(iii) ***Up-to-date information*** is essential if a customer needs to know, if a particular item is in stock. Argos stores have small key-pads in which a customer keys in a numerical stock codeto interrogate the database to check if the item is available.

(iv) ***Timely –*** Reports should be with the right person at the right time.

(v) ***Right level of detail –*** Often it is better to report only items that need action. Too much detail might make it hard to make sense. However, too little detail can lead to a simplistic response.

(vi) In an appropriate format, large tables of figures are meaningless.

Importance of Information

Information plays a very important role in management. It helps in management control, in decision-making, and in building models, backgrounds and motivation. In a business organization, the value of information is affected due to various factors like

completeness, timeliness, correctness, consistency, appropriateness, validity, usability, relevance and accessibility. Information can be justified or can be considered to have high value if its expected value is more than the costs of acquiring it. Information has a value when it has:

i) ***Surprise:*** The information tells me something I didn't know.

ii) ***Change in decision:*** This is decided something differently because of this new information.

iii) ***Payoff:*** The change results in an increased payoff.

iv) ***Information helps in management control:*** Information helps in ensuring proper management control. There are three types of control that exist in an organization. These are preliminary controls, screening controls and post action control. Preliminary controls ensure that the information is collected. Screening control ensures that the information is put to use in the right way. Post action control ensures that the gathered information reaches the right audience.

v) ***Information helps in decision-making:*** The process of decision-making is marked by a great deal of uncertainty and risk. Decisions in organizations are usually taken based on past experience and their outcome. Decision-making under certainty assumes perfect information as outcomes; risk assumes information as to the probability of each outcome. The person taking decision has to have good knowledge about various aspects and alternatives available. He should also have good knowledge about likely outcome in each of those alternatives. All these are possible only when the decision maker has the right information available. In decision theory, the value of information is the value of the change in decision behaviour caused by the information less the cost of obtaining the information.

Value of Information

Good quality information is accurate, up to date, and complete. However it does need to be passed through the right people with the right procedures if it is to have credibility. Credible information must have evidence to back it up. If it is to be acted on, it must be available at the right time. Following are the factors that affect the value of information:

(i) ***Detail*****:** The amount of detail must be sufficient to convey the information required but it must not be allowed to become excessive so that the meaning is obscured. Most people just want to be aware of the summary, although that does need to be based on relevant detail.

(ii) ***Purpose*****:** Information should be relevant for the purpose. A factory foreman will need to know the work assignment for each of the workers that he is responsible for. The managing director needs to know the productivity of each department.

(iii) ***Confidence*****:** To be credible, the information must be accurate, up to date and complete. It must be from a reliable source and be able to be evidenced. Without this, the user would notbe truly confident in its worth and would be reluctant to act on it. Sometimes, however, correct information does come from unreliable sources, but the lack of credibility may lead to its being ignored.

(iv) ***Format*****:** Large blocks of text with tables of figures do not make compelling reading

and even worse presentations.

(v) ***Style*****:** The way in which the information is presented is important. Too often people look forthe entertainment value in a presentation and there is the risk that it can be "dumped down". This can lead to the information losing its impact and being less authoritative.

(vi) ***Manner*****:** A report circulated informally may not have the same impact as a report presented ata formal meeting. However circulating a report before a meeting may well lead to more informed and productive discussion.

(vii) ***Timing*****:** If information is to be effective it must be presented at the right time. It must be available at a time when the knowledge gained from the information can be used to influence the decisions to be made.

(viii) ***Channel*****:** Information has to be sent using the proper procedures, so that, it can be checked where necessary.

(ix) ***Destination*****:** For information to be of use, it must reach the right person. This will be the person who has the power needed to make decisions based on the information.

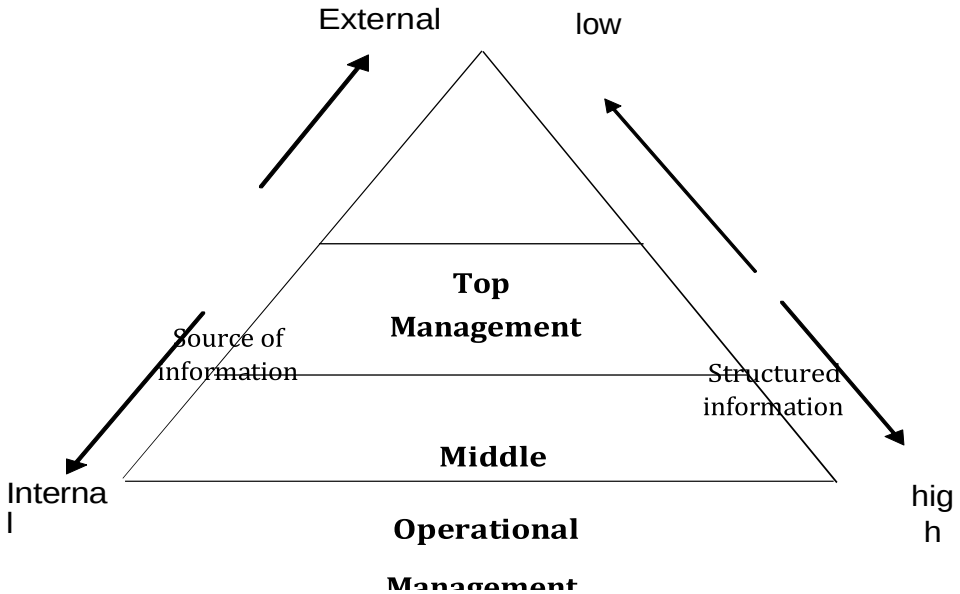
(x) ***Understandable*****:** Finally the information must be understandable. If all the above factors are present but the information itself is not understandable – perhaps because of the use of jargon, or bad grammar or axes missed off graphs then it will not be used.

Information and Management Level

Information provided to management must be relevant. It should not only relate to the particular manager's job, but also its level of detail should be appropriate. Information that is not relevant or that contains too little or too much detail will hinder the decision making process. Inthe early days of computers they were used for applications such as payrolls, where accurate calculation was important.

Information can be:

- At the operational level, for example, the day-to-day running of a business, such as payroll and invoicing.
- For middle management, tactical information is needed for effective management. Examples include how well a product is selling and whether a special promotion is needed.



- At the top level, senior managers need strategic information, such as new businesses opening up, employment patterns outside the company. These can build computer models on theinformation as well as historical company data to assess how well the company would perform if key strategic decisions were made.

Classification of Information

1. Based on Source

(i) ***Internal Information:*** The information gathered from within the organization is internal information. From within the organisation – possibly from data processing.

(ii) ***External Information:*** The information gathered from external agencies and external sources to the organization is external information. Possibly purchased or found in the public domain

(iii) ***Primary Information:*** Information from original data.

(iv) ***Secondary Information:*** Secondary data has been output by processing other data. Secondary data is not reliable as sometimes, because it has been processed from primary data that is notup to date.

2. Based on Nature

Based on nature, information can be classified into quantitative information, qualitative information, formal information and informal information.

(i) ***Quantitative Information:*** Quantitative information refers to information like numbers, statistics, scores etc., which is quantitative in nature. This information provides factual unbiased data. It is not biased or interpreted in light of personal opinions or experiences as it is quantifiable and can be measured.

(ii) ***Qualitative Information:*** Qualitative information refers to information which is gathered through personal and direct methods like personal interview, observation, case studies etc. Qualitative information is used for understanding the perceptions and interpretations of individuals and situations.

(iii) ***Formal Information:*** Formal information refers to the information which is presented in a structured format. Compared to informal information, formal information should be the roughly verified and checked for accuracy and reliability.

(iv) ***Informal Information:*** Informal information is presented in unstructured format. It is more casually presented and also is less reliable than formal information. *For example*, informal information in an organization is usually shared among employees through word of mouth, what usually is called as "grapevine".

3. Based on Level

(i) ***Strategic Information:*** Strategic information pertains mostly to the organisation as a whole and its environments, such as information about population changes, natural resources, new technologies, new products.

(ii) ***Tactical Information:*** Tactical information is required for short-term planning by middle level managers, sales analyses and forecasts, cash flow projections etc., are examples of tactical information.

(iii) ***Operational Information:*** Operational information relates to very short period that may be a few hours to a few weeks. It may be about current stock levels of inventory, outstanding orders from customers, work schedule for next shift etc.

4. Based on Application/Use

Based on application, information can be divided into planning information, control information and knowledge information.

(i) ***Planning Information:*** Specific rules, norms, standards and specifications that need to be adhered to while planning any activity. Hence, such information is called the planning information. The time standards, operational standards, the design standards are the examplesof planning information.

(ii) ***Control Information:*** The information that is used to put in place a feedback mechanism is called control information. Such information is used to compare the actual with the predetermined standards and to take corrective action wherever there are deviations.

(iii) ***Knowledge Information:*** This is the information collected through library reports and research studies. Such information is collected for building a knowledge base and may not directly influence decision-making.

5. Based on Structure/Type

Based on structure, information can be classified into detailed information, summarized information, sampled information and aggregated information.

(i) ***Detailed Information:*** Detailed information contains very specific details about a particular object, person, place, company or an issue. *For example*, information regarding the performance of a company over the years would provide detailed information about the company. However, using this information, one cannot make assumptions or arrive at

conclusions about other companies. Thus, this type of information provides all the information about a particular aspect.

(ii) ***Summarized Information:*** Summarized information comprises an outline of the total information. It is a summary of several items. Such information cannot be used for drawing conclusions about a single entity in the group. *For example*, the average amount of pocket money received by a teenager in Bangalore maybe Rs. 500 per month. However, there will be many teenagers in the city who receive much higher pocket money than just Rs. 500 and atthe same time there would be many who don't get the pocket money at all.

(iii) ***Sampled Information:*** Sampled information is a type of information which is obtained by examining a set of items that are randomly selected. *For example*, a product is tested in the market by distributing it to a set of selected customer base. The information obtained from such a test is called sampled information. The information assumes that the sample selected isa true representation of the entire population under consideration.

(iv) ***Aggregated Information:*** Aggregated information comprises every single bit of information about all the entities in a group. This information is very detailed in nature and is gathered from various data sources. Aggregated information is different from detailed information. Detailed information provides the details about a single entity in the group while aggregated information provides details about all the entities in the group. *For example*, an industry report on the textile industry would include the performance and contribution of the industry to the economy, the various players in the industry, their individual performance and respective contribution to the industry, etc. This is an aggregated information as one can find information about the entire textile industry as a whole as well as the detailed information about individual players in the industry.

6. Based on Time

(i) ***Historical Information:*** Information based on data collected over some period in the past e.g., sales figures for the past year. Whether or not information is historical depends on how quickly the underlying data is changing.

(ii) ***Current Information:*** Based on the latest data.

(iii) ***Future Information:*** Information based on predicted or possibly known future data values. Predicted data values could be based on current data modified by historical data. Sometimes predictions are little more than guesses and must be viewed with a great deal of care.

7. Based on Frequency

(i) ***Real Time Information:*** Real time information will be based on current data in a transaction processing application such as a supermarket. The information could be changed as the underlying data is updated. *For example,* at the start of the day there may be 42 bottles of a particular red wine in stock. Immediately a bottle is sold, the stock level is changed to one less.

(ii) ***Periodic Information:*** How often the information is put together – e.g., annual report, quarterly sales report. The longer the period, the more likely it is that the information will be strategic rather than operational.

8. Based on Form

The form that information is presented in will often be decided by the mechanism that is used to transmit it through the organisation.

(i) ***Written Information:*** Information is typed onto a piece of paper, a hard copy. It is low tech, but really quite reliable. The paperless office has been long promised but never delivered.

(ii) ***Visual Information:*** Presentation of sales trends in the form of a chart, or line graph.

(iii) ***Aural Information:*** At its simplest, this means listening to a senior person in the organisation droning on. You will find out that it's not just teachers who drone on. Aural presentation is often forgotten almost as soon as it's received. Some organisations record presentations onto tape so that people can listen to the tape while driving into work.

(iv) ***Sensory Information:*** Often when a new product is released, people in the organisation wantto see it, touch it, and feel it for themselves. Communication is often at its most effective if all the senses are involved.

9. Based on Flow of Information

Information can be classified into vertical and horizontal based on its flow within an organisation.

(i) ***Vertical Information:*** Information flowing up or down the organisation hierarchy is calledvertical information.

(ii) ***Horizontal Information:*** The information which is flowing opposite of vertical information iscalled horizontal information.

10. Other Classifications

(i) ***Action and No-action Information:*** Action information refers to information that induces some action while information that does not induce any action is called no-action information. *For example*, 'no stock' report calls for purchasing action while the stock ledge showing the store transactions and the stock balances is no-action information.

(ii) ***Recurring and Non-recurring Information:*** The information that is gathered at frequentintervals of time is recurring information e.g. monthly sales report while the information that is generated once at the end of any particular time period is non-recurring information, *for example*, the market research study conducted by the company would constitute non- recurring information as it may be conducted periodically.

Different between Data and Information

Sl. No.	Data	Information
1.	Data are facts, set of symbols to represent objects, events, activities and quantities.	Data arranged in certain order and form which is useful to the recipient is called Information.
2.	Data is raw materials.	Information is finished data
3.	Data always refers to facts.	Information is processed data, it never refers to facts.
4.	All data do not become information.	Information generates from data.
5.	Data are independent of users.	Information is user dependent.
6.	Data are unstructured.	Information is structured.
7.	Data are sometime meaningful.	Information must be meaningful.
8.	Data are the result of the routine recording of events which activities automatically.	Generation of information is user driven which is not always automatic.

CONCEPT OF SYSTEM

Meaning of System

The term system has been derived from Greek language System which means organized relationship among differentiated but associated elements. Existence of system is to achieve oneor more objectives of organisation which have been decided before designing of system.

A system is simply a group of activities and elements, which have been arranged to achievea certain objective. An information system is a combination of hardware, software and telecommunication systems, which can support business operations to increase productivity, and help managers make decisions.

Definition of System

According to ***Barry Boheam*** "A system is an orderly grouping in interdependent components linked together/according to a plan to achieve a specific objective."

According to ***Raymond Mcleod*** "A system is the set of elements in the form of ideas, things and people which are interrelated and part of a cohesive set-up, those synergies to achieve a specific goal or goals."

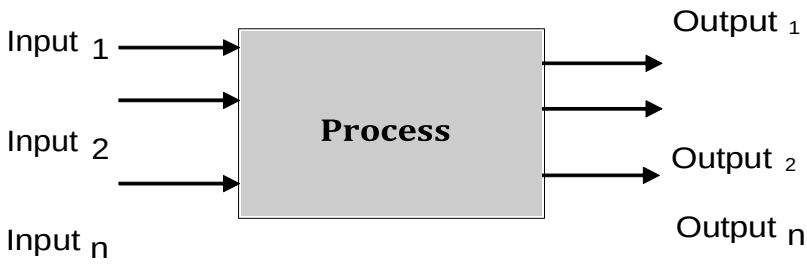
A System is a combination or arrangement of parts to form an integrated whole. System includes an orderly arrangement according to some common principles or rules.

A System is a scientific method of inquiry, that is, observation, the formulation of an idea, the testing of that idea and the application of the results.

Components of System

A simple system model is shown in the diagram below:

A system may have many inputs and outputs, as shown below :



As shown in the figure above, a system which has three basic interacting components or functions that is input, process and output is called as dynamic system.

The most common components of system are:

(i) Input (ii) Process (iii) Output

(iv) Feedback (v) Control (vi) Environment (vii) Boundary or Interface

(i) ***Input*****:** It involves capturing and assembling elements that enter the system to be processed,
for example, raw materials, money, labor, data etc.

(ii) ***Process*****:** Processing involves transformation process that converts input into output. For example manufacturing process, human breathing process etc.

(iii) ***Output*****:** It involves transferring elements that have been produced by the transformation process to their ultimate destination. *For example*, finished products, human services, information etc.

(iv) ***Feedback*****:** The feedback component gives feedback on the performance of the system. A negative feedback indicates that the system is deviating from its goal while a positive feedback indicates that the system performance is towards the achievement of the goal. It is a self regulatory.

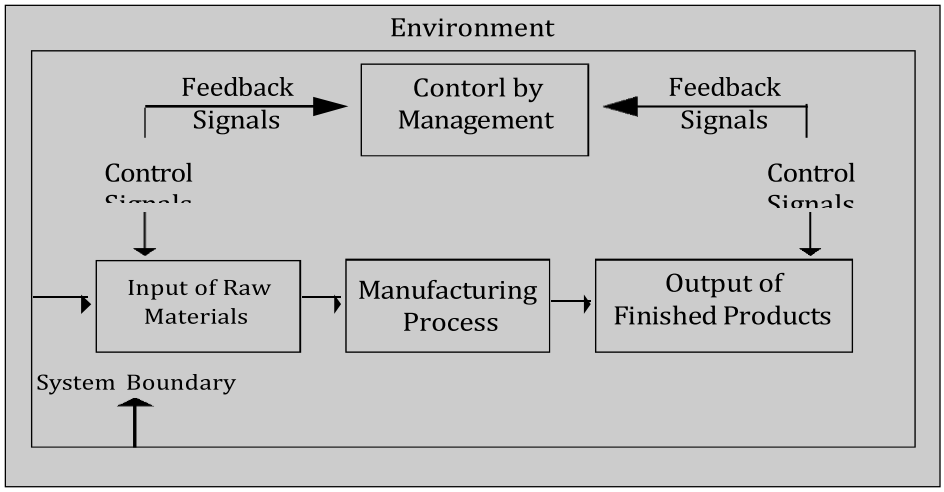
(v) ***Control*****:** The control component helps to take the corrective action, if required, to bring the system back towards the achievement of the system goal. It is a self monitoring system.

(vi) ***Environment*****:** A system does not exist in a vacuum, rather, it exists and functioning in an environment containing other systems. Several systems may share the same environment. If a system is one of the components of a large system, it is a

subsystem and the large system isits environment.

(vii) ***Boundary or Interface*****:** A system by defining its boundary, this means choosing which entities are inside the system and which are outside – part of the environment. Some of these systems may be connected to one another by means of a shared boundary or interface.

Similarly, manufacturing system is a system where raw materials are transformed by manufacturing processes into finished goods is shown below:



Characteristics of System

A system has following characteristics**:**

(i) ***Components*****:** A component is either an irreducible part or an aggregate of parts, also called a *subsystem*. The simple concept of a component is very powerful. *For example*, in case of an automobile we can repair or upgrade the system by changing individual components without having to make changes the entire system.

(ii) ***Organization*****:** Organization implies structure and order of the system. *For example*, the hierarchal relationship in a business organization/system represents the organization structure.

(iii) ***Interrelationships*****:** Interrelationships is the manner in which each component functions with other components of the system. *For example*, in a computer system, CPU must interact with input, output devices, main memory holds data and program and ALU does computation.

(iv) ***Boundary*****:** A system has a boundary, within which all of its components are contained and which establishes the limits of a system, separating it from other systems.

(v) ***Purpose or central objective*****:** Central Objective or Purpose means all components of a system assemble together towards a common goal, purpose or objective. The system's goal is the reason for its existence.

(vi) ***Environment*****:** A system operates within an environment – everything outside the system's boundary. The environment surrounds the system, both affecting it and being affected by it. *For example*, the environment of a university includes prospective students, foundations, funding agencies and the new media. Usually the system interacts with its environment. A

university interacts with prospective students by having open houses and recruiting from local high schools.

(vii) ***Interface*****:** The point at which the system meets its environment are called interface.

(viii) ***Constraints*****:** A system must face constraints in its functioning because there are limits to what it can do and how it can achieve its purpose within its environment. Some of these constraints are imposed inside the system (e.g., a limited number of staff available). Others are imposedby the environment (e.g., due to regulations). A system interact with the environment by means of inputs and outputs.

(ix) ***Input*****:** Input is *anything entering the system* from the environment.

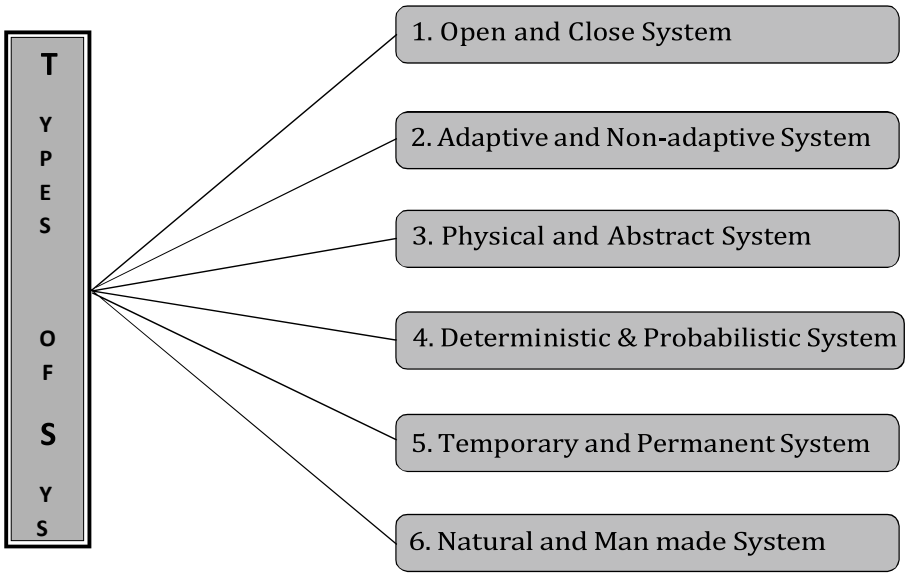
(x) ***Output*****:** Output is *anything leaving the system* crossing the boundary to the environment. Information, energy, and material can be both input and output in relation to the environment. People, *for example*, take in food, oxygen, and water from the environment as input. An electrical utility takes on input from the environment in the form of raw materials (coal, oil, water power, etc.), requests for electricity from customers. It provides for output to the environment in the form of electricity.

(xi) ***Interdependence*****:** Interdependence means how various components of the system depend on each other. Output of one system may be the input to another system.

(xii) ***Integration*****:** Integration means how a system is tied together. Components of a system may work independently and each component performs a unique function but they have to work together within the system to achieve the system goals

Types of System

Systems can be classified into a number of categories which are given below:



1. Open and Close System

Based on the degree of independence, systems can be classified as open and close system. An open system is one which interacts with its environment. It has many interfaces with its environment. An open system is influenced by its environment and has exchanges with the environment. *For example*, an educational institution affiliated to bangalore university is an open system because it has interaction with university and gets influenced by any changes in the university norms. On the contrary, a close system does not interact with its environment. It doesn't accept or provide any inputs or outputs to the external environment.

2. Adaptive and Non-adaptive System

A system that reacts to its environment in such a way as to improve its functioning, achievement or probability of survival is called an adaptive system. For the success of the business, the organizations need to change and adapt to the changing environment, like they need to change as per the changing customer demands. Today computers are a non-adaptive systems because if computers learn how to modify and upgrade themselves, then they would become an adoptive system.

3. Physical (Empirical) and Abstract (conceptual) System

Abstract systems are concerned with theoretical structures. They are systems of explanation. A conceptual system is an orderly arrangement of ideas. A physical or empirical system is a set of tangible entities that may be static or dynamic and operates together to accomplish an objective. Physical systems may be derived from or based upon conceptual systems and thus represent the conversion of concepts into practice.

4. Deterministic and Probabilistic System

A deterministic system operates in a predictable manner. It is a system where inputs, process and outputs are known with certainty. If the given state of the system and all possible operations are known, then the next state may be determined or predicted. For example an accounting system, a computer program; both these systems performs exactly according to a setof instructions. A probabilistic system is one whose exact state at any given time cannot be predicted. An inventory system is an example of probabilistic system. The average demand, average time for replenishment etc., may be defined but the exact value at any given time is not known.

5. Temporary and Permanent Systems

The policies of a business operation are permanent as far as year-by-year operations are concerned. A small group-research project in the laboratory is temporary. Very less man-made systems are permanent. Truly temporary systems are designed to last a specified period of time and then dissolve.

6. Natural and man-made Systems

There are natural and man-made systems. Natural systems may not have an apparent objective but their outputs can be interpreted as purposes. Man-made systems are made with purposes that are achieved by the delivery of outputs. Their parts must be related; they must be "designed to work as a coherent entity" - else they would be two or more distinct systems.

CONCEPT OF INFORMATION SYSTEM

An information system is an organized combination of people, hardware, software, communications networks and data resources that collects, transforms and disseminates information, to support decision making and control in an organization.

In addition to supporting decision making and control, information system may also help managers in coordination, analyze problems, create new products etc.

Meaning of Information System

An Information System (IS) is a collection of interrelated components that collect, process, store and provide as output the information needed to complete a business task.

Example: A payroll system, for example, collects information on employees and their work, processes and stores that information and then produces pay checks and payroll reports for the organization. Then information is provided to manufacturing so the department can schedule production.

Importance of Information System

(i) Information system supports – (a) Business processes and operations (b) Business decisionmaking and (c) Strategies for competitive advantage.

(ii) Information system plays a vital role in the e-business and e-commerce operations.

(iii) Information system maintains enterprise collaboration and management and strategic successof business through internet, which is worked global environment.

Functions of Information System

Functions of information system are describing below:

(i) Information system help managers, works analysis problems, visualize complex subjects andcreate new products.

(ii) Information system will contain information about people, place and things with theorganization.

(iii) It will contain data that have been shaped into a form, which are meaningful and useful tohuman beings.

(iv) Information system will produce information so that organizations will take decisions, controloperators and analyze problems.

(v) Information system will encompass the understanding of the management and organizationaldimensions of system.

(vi) Information system is used for building and managing system.

(vii) Information system designates a specific category of serving management level functions.

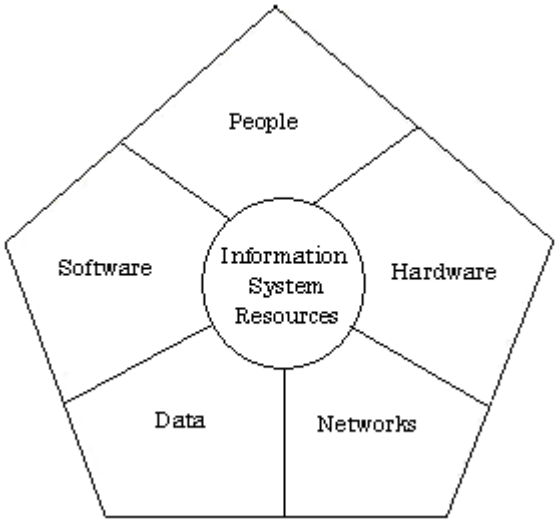
(viii) Information system is saving as foundation for new services and products.

Component of Information System

The physical components of any Information System are:

1. People Resources

People are required for the operation of all information systems. These people resources include end users and ARE specialists. End users (also called users or clients) are people whouse an information system or the information it produces. They can be accountants, salespersons, engineers, clerks, customers or managers. Most of us are information system end users.



2. Hardware Resources

The concept of Hardware resources includes all physical devices and materials used in information processing. Specially, it includes not only machines, such as computers and other equipment, but also all data media, that is, all tangible objects on which data is recorded, from sheets of paper to magnetic disks. Example of hardware in computer-based information systems are:

Computer systems, which consist of central processing units containing microprocessors, and variety of interconnected peripheral devices. Examples are microcomputer systems, midrange computer systems and large mainframe computer systems.

Computer peripherals, which are devices such as a keyboard or electronic mouse for input of data and commands, a video screen or printer for output of information, and magnetic or optical disks for storage of data resources.

3. Software Resources

The concept of Software Resources includes all sets of information processing instructions. This generic concept of software includes not only the sets of operating instructions called programs, which direct and control computer hardware, but also the sets of information processing instructions needed by people, called procedures.

It is important to understand that even information systems that don't use computers have a software resource component. This is true even for the information systems of ancient times, or the manual and machine-supported information systems still used in the world today. They all require software resources in the form of information processing instructions and procedures in order to properly capture, process, and disseminate information to their users.

4. Data Resources

Data is more than the raw material of information systems. The concept of data resources has been broadened by managers and information systems professionals. They realize that data constitutes a valuable organization resource. Thus, you should view data as data resources that must be managed effectively to benefit all end users in an organization.

Data can take many forms, including traditional alphanumeric data, composed of numbers and alphabetical and other characters that describe business transactions and other events and entities. Text data, consisting of sentences and paragraphs used in written communications; image data, such as graphic shapes and figures and audio data, the human voice and other sounds, are also important forms of data.

Example: Names, quantities, and dollar amounts recorded on sales forms represent data about sales transactions. However, a sales manager may not regard these as information. Only after such facts are properly organized and manipulated can meaningful sales information be furnished, specifying, for example, the amount of sales by product type, sales territory, or sales persons.

5. Network Resources

Telecommunications networks like the Internet, intranets, and extranet have become essential to the successful operations of all types of organizations and their computer-based information systems. Telecommunications networks consist of computers, communications processors, and other devices interconnected by communications media and controlled by communications software. The concept of Network resources emphasizes that communications

networks are a fundamental resource component of all information systems. Network resources include:

Communication media, Examples include twisted pair wire, coaxial cable, fiber-optic cable, microwave systems, and communication satellite systems.

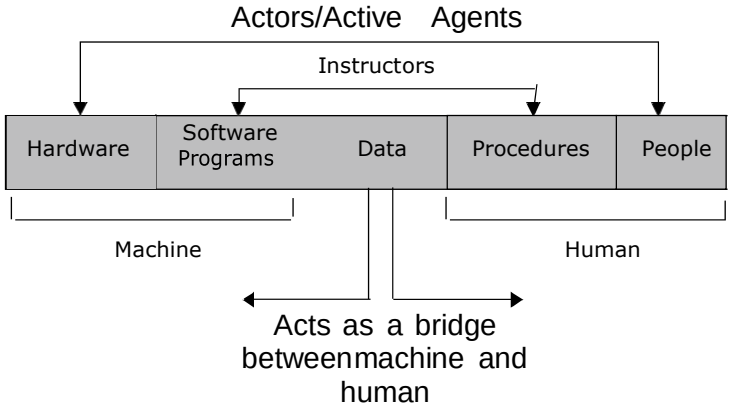
Network Support, This generic category includes all of the people, hardware, software and data resources that directly support the operation and use of a communications network. Examples include communications control software such as network operating systems and Internet packages.

COMPUTER BASED INFORMATION SYSTEM

Computer based information system is an organized integration of hardware and software technologies and human elements designed to produce timely, integrated, accurate and useful information for decision making purposes. Computer Based Information System (CBIS) is an information system in which the computer plays a major role.

Elements of Computer Based Information System

Computer Based Information System consists of the following elements:



1. ***Hardware:*** The term hardware refers to machinery. This category includes the computeritself, which is often referred to as the central processing unit (CPU), and all of its support equipments. Among the support equipments are input and output devices, storage devices and communications devices.
2. ***Software:*** The term software refers to computer programs and the manuals (if any) that support them. Computer programs are machine-readable instructions that direct the circuitry within the hardware parts of the Computer Based Information System (CBIS) to function in ways that produce useful information from data. Programs are generally stored on some input/ output medium-often a disk or tape.
3. ***Data:*** Data are facts that are used by program to produce useful information. Like programs, data are generally stored in machine-readable from on disk or tape until the computer needs them.

4. ***Procedures:*** Procedures are the policies that govern the operation of a computer system. Procedures are to people what software is to hardware" is a common analogy that is used to illustrate the role of procedures in a CBIS.
5. ***People:*** Every Computer Based Information System (CBIS) needs people if it is to be useful. Often the most over-looked element of the CBIS is the people: probably the components that most influence the success or failure of information system.

INFORMATION TECHNOLOGY

Meaning of Information Technology

Information Technology refers to the branch of engineering that deals with the use of computers and telecommunications to retrieve and store and transmit information. It is the combination of systems, procedures, software, and hardware involved in establishing an effective and leading-edge methodology for enabling a total supply chain network of response - from incoming materials through delivery and satisfaction with finished goods and services.

Role of IT in various sectors

1. Education

Getting the right kind of information is a major challenge as is getting information to make sense. College students spend an average of 5-6 hours a week on the internet. Research shows that computers can significantly enhance performance in learning. Students exposed to the internet say they think the web has helped them improve the quality of their academic researchand of their written work. One revolution in education is the advent of distance learning. This offers a variety of internet and video-based online courses.

2. Health and Medicine

Computer technology is radically changing the tools of medicine. All medical informationcan now be digitized. Software is now able to computer the risk of a disease. Mental health researchers are using computers to screen troubled teenagers in need of psychotherapy. A patient paralyzed by a stroke has received an implant that allows communication between his brain and a computer; as a result, he can move a cursor across a screen by brain power and convey simple messages.

3. Science

Scientists have long been users of it. A new adventure among scientists is the idea of a "collaboratory", an internet based collaborative laboratory, in which researchers all over the world can work easily together even at a distance. An example is space physics where space physicists are allowed to band together to measure the earth's ionosphere from instruments on four parts ofthe world.

4. Business

Business clearly sees the interest as a way to enhance productivity and competitiveness. Some areas of business that are undergoing rapid changes are sales and marketing, retailing, banking, stock trading, etc. Sales representatives not only need to be better educated and more knowledgeable about their customer's businesses, but also must be comfortable with computer technology. The internet has become a popular marketing tool. The world of cyber cash has come to banking – not only smart cards but internet banking, electronic deposit, bill paying, online stock and bond trading, etc.

Advantages of Information Technology

The advantages of Information Technology can be summarized as follows:

1. Globalization

True globalization has come about only via this automated system. The creation of one interdependent system helps us to share information and end linguistic barriers across the continents. The collapse of geographic boundaries has made the world a 'global village'. The technology has not only made communication cheaper, but also possible much quicker and round the clock. The wonders of text messages email and auto-response, backed by computer security applications, have opened up scope for direct communication.

2. Cost-effective

Computerized, internet business processes have made many businesses turn to the Internetfor increased productivity, greater profitability, clutter free working conditions and global client. It is mainly due to the IT industry that business has been able to make their processes more streamlined, thereby becoming more cost-effective and consequently more profitable. People are able to operate their businesses 24x7, even from remote locations only due to the advent of information technology.

3. Communication

Quick and effective communication is vital to any business anywhere in the world. Information technology gives an entrepreneur or business the tools, like email, video conferencing, SMS, etc., essential to communicate efficiently and effectively. To the business world, and information technology gives your company the resources it needs to communicate quickly and effectively. Not only do people connect faster with the help of information technology, but they are also able to identify like-minded individuals and extend help, while strengthening ties.

4. Storing and Protecting Information

IT provides a low-cost business options to store and maintain information that may be important from a business or service point of view. Virtual vaults and other such security systems not only store vital data but also allow control over the access to such information. IT

security systems will also protect virtual data from being hacked or wiped out in case of anytechnical failure.

5. Creation of New Jobs

One of the biggest advantages of IT has been the creation of a whole new field of opportunity for skilled personnel leading to new and interesting jobs. Hardware and software developers, computer programmers, web designers, system analyst, the list of new jobs created could go on. IT has also been attributed to be the major cause of surge in the economies of certain Third World nations too. Things that were once done manually or by hand have now become easier and faster due to the advent of a computing technology. Our world today has changed a great deal with the aid of IT which has penetrated almost every aspect of our daily lives and society, from leisure to business. IT has become a part of our day-to-day lives throughthe evident use of PC's, Internet, cell phones, faxes, the list would seem endless. Let us hope that newer development in the field of IT can provide benefits to our future generations, just as it has greatly benefited ours.

Disadvantages of Information Technology

The disadvantages of Information Technology can be summarized as follows:

1. ***Over reliance on technology*** - a lot of people believe that because computers and the Internet has become such a regular part of modern life, some people particularly children who grow up with it, will not be able to function without it. Some people think that the Internet is making people lazy, particularly when it comes to essay or project research as instead of reading books in a library, one can just perform a Google search.
2. ***Loss of communication skills -*** with the ever increasing variety of social networking sites such as Face book and Twitter, a lot of people are worried that traditional communicationskills will be lost. This worry is particularly about children who often engage in these websites because communication and interactive skills are not important with computers.
3. ***Job losses -*** technology in an organization, company or business, the number of hours that a human works at that company are reduced. This may even result in some people losing their jobs because technology is doing it for them. However this is beneficial for the organization as their profit is increased because they don't need to pay their workers as much because they aren't required as much.
4. ***Loss of personal touch*** - emails and instant messaging have replaced the old tradition of handwriting letters. And although this is advantageous because of time constraints, a personal touch and sense of feeling is lost compared to taking the time to sit down and hand write a letter.
5. ***Health problems -*** research has shown that technology can cause a number of problems with a person's health. Many scientists, doctors and researchers are concerned about possible links between technology and heart problems, eye strain, obesity, muscle problems and deafness.

Waste emitted from technology can pollute the environment which not only makes people ill, italso damages the environment.

IMPACT OF INFORMATION TECHNOLOGY ON BUSINESS

The rise of information technology has paved the way for various innovations. With the digitization of information, more and more businesses are increasingly leveraging the benefits of digital tools to improve their prospects. Information technology has been crucial in turning this process into a complete success. Information technology has dramatically transformed the lives of individuals. It provides businesses the scope to analyze data and plan business strategies accordingly. Utilizing information technology means that the data analysis is accurate, thus optimizing profits.

Business Data Processing

Business data processing includes all operations performed on data a disclosure, management, use and collection of data are four examples of business data processing within a company. The strategic goal of data processing is to convert raw data into meaningful information that improves a current situation or resolves an existing problem. Data processing outputs often take various forms such as reports, diagrams and graphics that make the data easier to understand and analyze.

Steps in Business Data Processing

In a complete data processing operation, you should pay attention to what is happening infive distinct business data processing steps:

Step-1: ***Editing:*** What data do you really need? Extracting and editing relevant data is thecritical first step on your way to useful results.

Step-2: ***Coding:*** This step is also known as bucketing or netting and aligns the data in asystematic arrangement that can be understood by computer systems.

Step-3: ***Data Entry:*** Entering the data into software is a step that can be performedefficiently by data entry professionals.

Step-4: ***Validation:*** After a “cleansing” phase, validating the data involves checking (andpreferably double-checking) for desired quality levels.

Step-5: ***Tabulation:*** Arranging data in a form that facilitates further use and analysis.

Intra and Inter-organizational communication by using network technology

Inter-communication takes place “outside” – in other words, it is in the open domainand may be considered in the three ways below:

– Inter-personal communication involves the exchange of message/information/data acrosscommunication channel from one person to another or one group to another.

– Inter-organizational communication describes communication between separate organizations – for example, a negotiation for a long-term business agreement such as a supplierand development chain or network.

– Internet communication uses a computer-based system that is open to the users – e.g. World-Wide-Web. Individuals and companies are able to buy, sell, advertise, investigate – in fact, conduct all manner of communication processes – in a way that might be person-to-person, person-to company or company-to-company.

Intra-communication takes place "inside" the individual/body/group/network/organization and may be considered in the three ways below:

– Intra-personal communication takes place "inside" the person; the process of intra- personal communication involves the transmission of data/information/feelings between the various senses or pathways.

– Intra-organizational communication classifies communication that is internal within theorganization: it describes the use of company magazines or newsletters which are used as the communication channel.

– Intranet communication is a form of communication channel using computer-based technology harnessed by the organization to allow internal communication to take place – eg an internal email network.

BUSINESS PROCESS OUTSOURCING

Business process outsourcing (BPO) is the contracting of non-primary business activities and functions to a third-party provider. BPO services include payroll, human resources (HR), accounting and customer/call center relations.

BPO is also known as Information Technology Enabled Services (ITES). Often the business processes are information technology-based and are referred to as ITES-BPO, where ITES stands for Information Technology Enabled Service.

BPO Business Process Outsourcing services can be divided into back office outsourcing and front office outsourcing. Back Office Outsourcing services can include quality assurance, data entry, data management, accounting support, payment processing and surveys. Front Office Outsourcing services can include fax, email, phone conversations and other forms of communication with customers. Companies will typically outsource BPO front office services in customer service/support, inbound and outbound sales, market research, appointment scheduling, and technical support.

Benefits and Advantages of Business Process Outsourcing

1. ***Cost Reduction:*** If somehow you have stumbled upon the need for BPO services, it is likely you are looking to continue to build the integrity of your business. In this case, BPO can offer your organization a financial strategy to cut cost without having to sacrifice quality.

2. ***Focus on your Business:*** Most business that seek Business Process Outsourcing BPO services are looking to expand their current products and services but do not have the time or resources to do so. BPO services can offer organizations the opportunity to free up the time to focus on their core offerings.
3. ***Improved Productivity:*** For the most part, BPO Companies have worked on their craft, mastered their process and are actively working with the best technology and resources. By doing so, they can draw the most optimal performance and productivity out of their workforce.
4. ***Access to state of the art process and technology resources:*** Some of the perks of outsourcing services to a BPO company know you are in the right hands. BPO companies are constantly working on improving their workforce and facilities by adopting the most recent technologies, practices and assets to run an even more improved machine. Events can be a great way to build local, national and global ventures and ultimately, build tech communities along the way.
5. ***Ability to reassign resources:*** If you have decided to jump on board with BPO services, you will more than likely have resources working in the mail, printing, check writing, rebate fulfillment and other paper-driven tasks. By choosing a BPO provider you can reallocate resources, cut cost on task and use either office or warehouse space for additional improvements.

KNOWLEDGE PROCESS OUTSOURCING

Knowledge Process Outsourcing (KPO) describes the outsourcing of core information- related business activities which are competitively important or form an integral part of a company's value chain. KPO requires advanced analytical and technical skills as well as a high degree of specialist expertise.

Importance of Knowledge Process Outsourcing (KPO)

1. In the present day world almost all the businesses are information driven. Information has become an essential part of any business, which helps them to offer innovative products andto serve the customer in a better manner.
2. With the increased importance of information in business, the Knowledge Process Outsourcing service providers are now looked upon by the organizations for meaningful information that will promote business growth. This is true in the case companies operating in the retail sector too.
3. KPO service providers provide all the information required to start a business and to run it successfully.
4. The KPO service providers help retail businesses to find out solutions to the most difficult questions they face in their business.
5. KPO will give them answers regarding the reasons for decline in market share, whether the pricing of the products or services is proper etc.

6. Knowledge Process Outsourcing service providers provide advanced analytics solutions that include study of customer behavior, their mind and habits. The information provided by such service providers will include the buying behavior of customers, their preferences and patterns, information about the market, sales forecast and information on the market share.
7. Service providers may even make use of predictive modeling to create meaningful and actionable insights into consumer behavior.
8. They also provide innovative solutions such as competitive intelligence solutions which help clients to track their competitors on their pricing and launching of new products.
9. The services provided by KPO firms help clients to handle their business in a better manner. The information provided by the KPO firms will help clients to manage their products and brand better than competitors.
10. Moreover they help firms to improve the brand image of the clients business with proper marketing techniques and practices.
11. The information provided by the KPO firms will help clients to better handle their vendors and customers in real time. It will also help in reducing the operational cost and thus streamline the business activities, which increases the efficiency of the business.
12. Thus with wide range of services offered by KPO firms, the clients will be able to make their business more attractive and productive.

Challenges of Knowledge Process Outsourcing (KPO)

Major Challenges of Knowledge Process Outsourcing (KPO) are as follows:

1. The challenges of pursing a KPO strategy are both external and internal.
2. External challenges include finding a suitable KPO vendor that can offer the necessary skills in a scalable manner.
3. Protecting intellectual property is a challenge since it will have to be shared with the vendor. For some industries, protecting data and privacy as well as abiding to legal and compliance requirements are challenges to overcome.
4. The physical location of the KPO vendor creates challenges from a language and time zone perspective. Internal challenges stem from adapting the organizational and management mindset from managing internal resources to managing the KPO vendors resources situated ina remote location.
5. The definition of quality and performance metrics can pose a challenge since some of them may not exist.
6. Internal processes and managers usually do not have quality metrics in place and will need tobe defined before outsourcing the process.
7. In some cases, the outsourcing effort exposes inefficiencies and weak areas in the process and a decision needs to be made to outsource the process as is or to optimize it before outsourcing.

A database is an organized collection of data. It is considered as a container of information.

In the manual system, you would maintain several files with different bits of information while in the computerized system you would use database programs such as Microsoft Access, OpenOffice.org Base, and MySQL, to organize the data as per your business need.

Database Management System :

A database management system is a software package with computer programs that controls the creation, maintenance, and use of a database. for example Oracle, IBM DB2, Microsoft SQL Server, Microsoft Access, PostgreSQL, MySQL, FoxPro, and SQLite.

Data can be organized into two types:

1. **Flat File : Data is stored in a single table. Usually suitable for less amount of data.**
2. **Relational : Data is stored in multiple tables and the tables are linked using a common field. Relational is suitable for medium to large amount of data.**

Database Servers :

Database servers are dedicated computers that hold the actual databases and run only the DBMS and related software.

Advantages of Database :

1) Reduces Data Redundancy : Database reduces data redundancy (duplication of data)
2) Sharing of Data : In a database, the users of the database can share the data among themselves.
3) Data Integrity : Data integrity means that the data is accurate and consistent in the database.

4) Data Security : Database provides data security as only authorized users are allowed to access the database and their identity are authenticated by using a username and password.
5) Privacy : The privacy rule in a database states that only the authorized users can access a database according to its privacy constraints.
6) Backup and Recovery : Database Management System automatically takes care of backup and recovery.

Some key features of a database:

1) A database can have one or many tables.

2) Each table in a database contains information about one type of item.

3) Every table has a key field which ensures that there are 100% unique values throughout the database.

Important Terms :

1) Primary Key : A primary key is a unique value that identifies a row in a table. It helps the database to search for a record.
2) Composite Primary Key : When primary key constraint is applied on one or more columns then it is known as Composite Primary Key.
Data in a relational database management system (RDBMS) is organized in the form of tables.

DATABASE OBJECTS :

1) Table : A table is a set of data elements (values) that is organized using a model of vertical columns and horizontal rows.
2) Columns or Fields or Attributes: A column is a set of data values of a particular simple type, one for each row of the table.

Unit 3: Internet and Its Applications [8 Marks, Class: 8]

What is the Internet?

Answer: A global system of interconnected computers, using a standardised Internet Protocol suite for communication and sharing information is called the Internet.

What is ISP?

Answer: ISP stands for Internet Service Provider. This helps in providing direct access for using the internet from your office or home, connected through landlines. With the introduction of Wi-fi and broadband, connecting to the Internet has become wireless.

What is the World Wide Web?

Answer: World Wide Web or 'www' is a collection of webpages which can easily be published on the Internet and read by millions of its users.

Question: What is an IP address?

Answer: The Internet Protocol address is a numerical identification code assigned for any device connected to a network. It acts as an identification interface for Internet users.

What is a Web Browser?

Answer: A web browser is a software application for accessing the information on the World Wide Web. The commonly used web browsers include Google Chrome, Internet Explorer, Mozilla Firefox, etc.

Ways To Connect To Internet

The different ways in which one can connect to the Internet are discussed below in brief:

- **Dial-Up –** In such connections, users are required to link their phone line to a computer to access the Internet. Under this connection, the user cannot make or receive phone calls through tier home phone service
- **Broadband –** Provided either through cable or phone companies, Broadband is a high-speed internet connection which is widely used today
- **Wireless Connection –** Wi-fi and Mobile service providers fall under this category. Internet connectivity is made via radio waves and the Internet can be connected anywhere, irrespective of the location. Given below are a few examples of wireless connection:
    - **Wi-fi –** Wireless Fidelity or wi-fi allows high-speed internet connectivity without the use of wires
    - **Mobile Phones –** All smartphones are now equipped with an option for Internet connectivity which can be availed using Internet vouchers and packs. No external connection or wire is required for these
    - **Satellite –** Where broadband connections are unavailable, satellites are used for wireless Internet connectivity
    - **Integrated Services Digital Network –** ISDN allows users to sent audio or video data using telephone lines

Internet Connection Protocols

Protocols are a set of rules that help in governing the way in which any particular body or technology works.

Internet Connection Protocols can be divided into three major types:

- **TCP/IP Network Model –** Transmission Control Protocol (TCP) and Internet Protocol (IP) are the most widely used protocols for connecting networks. It divides any message into a series of packets which are sent from source to destination

- **File Transfer Protocol –** Program files, multimedia files, text files, documents, etc. can be transferred from one device to another, using FTP
- **Hypertext Transfer Protocol –** Used for transferring a hypertext from one device to two or more devices. HTML tags are used for creating links and these links may be in the form of text or images

- **What is HTML?**
- HTML is the markup language which helps you to create and design web content. It has a variety of tag and attributes for defining the layout and structure of the web document. It is designed to display data in a formatted manner. A HTML document has the extension .htm or .html.

- **What is XML?**
- XML is a markup language which is designed to store data. It is popularly used for the transfer of data. It is case sensitive. XML offers you to define markup elements and generate customized markup language. The basic unit in the XML is known as an element. Extension of XML file is .xml
- **CLOUD COMPUTING & IO**T

The cloud is a huge, interconnected network of powerful servers that performs services for businesses and people. The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT has evolved with the greater generation of data. Internet of Things Cloud Service creates excessive communication between inexpensive sensors in the IoT which means even greater connectivity. Billions of connected devices and machines will soon join human-users. IoT generates lots of data while on the other hand, cloud computing paves way for this data to travel. In this paper we try to focus on cloud providers who take advantage of this to provide a pay-as-you-use model where customers pay for the specific resources used. Also, cloud hosting as a service adds value to IoT startups by providing economies of scale to reduce their overall cost structure.

Unit 4: Security and Encryption [8 Marks, Class: 8]

Viruses, worms, Trojans, and bots are all part of a class of software called "malware." Malware is short for "malicious software," also known as malicious code or "malcode." It is code or software that is specifically designed to damage, disrupt, steal, or in general inflict some other "bad" or illegitimate action on data, hosts, or networks.

There are many different classes of malware that have varying ways of infecting systems and propagating themselves. Malware can infect systems by being bundled with other programs or attached as macros to files. Others are installed by exploiting a known vulnerability in an operating system (OS), network device, or other software, such as a hole in a browser that only requires users to visit a website to infect their computers. The vast majority, however, are installed by some action from a user, such as clicking an email attachment or downloading a file from the Internet.

Some of the more commonly known types of malware are viruses, worms, Trojans, bots, ransomware, backdoors, spyware, and adware. Damage from malware varies from causing minor irritation (such as browser popup ads), to stealing confidential information or money, destroying data, and compromising and/or entirely disabling systems and networks.

In addition to damaging data and software residing on equipment, malware has evolved to target the physical hardware of those systems. Malware should also not be confused with defective software, which is intended for legitimate purposes but contains errors or "bugs."

Classes of Malicious Software

Two of the most common types of malware are viruses and worms. These types of programs are able to self-replicate and can spread copies of themselves, which might even be modified copies. To be classified as a virus or worm, malware must have the ability to propagate. The difference is that a worm operates more or less independently of other files, whereas a virus depends on a host program to spread itself. These and other classes of malicious software are described below.

Ransomware

Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called *cryptoviral extortion*, which encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Viruses

A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels. Viruses can range in severity from causing mildly annoying effects to damaging data or software and causing denial-of-service (DoS) conditions. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program. When the host code is executed, the viral code is executed as well. Normally, the host program keeps functioning after it is infected by the virus. However, some viruses overwrite other programs with copies of themselves, which destroys the host program altogether. Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected email attachments.

Worms

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them. A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided. More advanced worms leverage encryption, wipers, and ransomware technologies to harm their targets.

Trojans

A Trojan is another type of malware named after the wooden horse that the Greeks used to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojans are also known to create backdoors to give malicious users access to the system. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. Trojans must spread through user interaction such as opening an email attachment or downloading and running a file from the Internet.

Bots

"Bot" is derived from the word "robot" and is an automated process that interacts with other network services. Bots often automate tasks and provide information or services that would otherwise be conducted by a human being. A typical use of bots is to gather information, such as web crawlers, or

interact automatically with Instant Messaging (IM), Internet Relay Chat (IRC), or other web interfaces. They may also be used to interact dynamically with websites.

Bots can be used for either good or malicious intent. A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet." With a botnet, attackers can launch broad-based, "remote-control," flood-type attacks against their target(s).

In addition to the worm-like ability to self-propagate, bots can include the ability to log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch Denial of Service (DOS) Attacks, relay spam, and open backdoors on the infected host. Bots have all the advantages of worms, but are generally much more versatile in their infection vector and are often modified within hours of publication of a new exploit. They have been known to exploit backdoors opened by worms and viruses, which allows them to access networks that have good perimeter control. Bots rarely announce their presence with high scan rates that damage network infrastructure; instead, they infect networks in a way that escapes immediate notice.
Advanced botnets may take advantage of common internet of things (IOT) devices such as home electronics or appliances to increase automated attacks. Crypto mining is a common use of these bots for nefarious purposes.

Distribution Channels for Malware

Advanced malware typically comes via the following distribution channels to a computer or network:

- Drive-by download—Unintended download of computer software from the Internet
- Unsolicited email —Unwanted attachments or embedded links in electronic mail
- Physical media—Integrated or removable media such as USB drives
- Self propagation—Ability of malware to move itself from computer to computer or network to network, thus spreading on its own

For a complete listing of malware tactics from initial access to command and control, see MITRE Adversarial Tactics, Techniques, and Common Knowledge.

Ten Best Practices for Combating Malware

1. Implementing first-line-of-defense tools that can scale, such as cloud security platforms
2. Adhering to policies and practices for application, system, and appliance patching
3. Employing network segmentation to help reduce outbreak exposures
4. Adopting next-generation endpoint process monitoring tools
5. Accessing timely, accurate threat intelligence data and processes that allow that data to be incorporated into security monitoring and eventing
6. Performing deeper and more advanced analytics
7. Reviewing and practicing security response procedures
8. Backing up data often and testing restoration procedures—processes that are critical in a world of fast-moving, network-based ransomware worms and destructive cyber weapons
9. Conducting security scanning of microservice, cloud service, and application administration systems
10. Reviewing security systems and exploring the use of SSL analytics and, if possible, SSL decryption

Advanced Persistent Threats (APT)

A set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity. An APT usually targets either private organizations, states, or both for business or political motives. APT processes require a high degree of covertness over a long period of time. The "advanced" process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The "persistent" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack.

Adware

Software that generates revenue for its developer by automatically generating online advertisements in the user interface of the software or on a screen presented to the user during the installation process. The software may generate two types of revenue: one is for the display of the advertisement and another on a "pay-per-click" basis if the user clicks on the advertisement.

Backdoor

An undocumented way of accessing a system, bypassing the normal authentication mechanisms. Some backdoors are placed in the software by the original programmer and others are placed on systems through a system compromise, such as a virus or worm. Usually, attackers use backdoors for easier and continued access to a system after it has been compromised.

Bootkit

A malware variant that modifies the boot sectors of a hard drive, including the Master Boot Record (MBR) and Volume Boot Record (VBR). Adversaries may use bootkits to persist on systems at a layer below the operating system, which may make it difficult to perform full remediation unless an organization suspects one was used and can act accordingly.

Browser Hijacker

Software that modifies a web browser's settings without a user's permission to inject unwanted advertising into the user's browser. A browser hijacker may replace the existing home page, error page, or search engine with its own. These are generally used to force hits to a particular website, increasing its advertising revenue. This software often comes in the form of a browser toolbar and is received through an email attachment or file download.

Crimeware

A class of malware designed specifically to automate cybercrime. Crimeware (distinct from spyware and adware) is designed to perpetrate identity theft through social engineering or technical stealth in order to access a computer user's financial and retail accounts for the purpose of taking funds from those accounts or completing unauthorized transactions that enrich the cyberthief. Alternatively, crimeware may steal confidential or sensitive corporate information.

Denial of Service (DOS) Attacks

Malicious attempts by one or more people to cause the victim, site, or node to deny service to its customers.

Executable File

A computer file that contains a sequence of instructions to run an automatic task when the user clicks the file icon or when it is launched via a command.

Exploit

A piece of software, a command, or a methodology that attacks a particular security vulnerability. Exploits are not always malicious in intent—they are sometimes used only as a way of demonstrating that a vulnerability exists. However, they are a common component of malware.

Instant Messaging

Applications for personal or business communication that are built around the concept of online presence detection to determine when an entity can communicate. These applications allow for collaboration via text chat, audio, video or file transfer.

Internet Relay Chat

A system for chatting that involves a set of rules and conventions and client/server software.

Keyloggers

The action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program. A keylogger can be either software or hardware.

Malicious Crypto Miners

Software that uses system resources to solve large mathematical calculations that result in some amount of cryptocurrency being awarded to the solvers. There are two ways that mining can be performed: either with a standalone miner or by leveraging mining pools. Mining software relies on both CPU resources and electricity. Once a system has a miner dropped on it and it starts mining, nothing else is needed from an adversary perspective. The miner generates revenue consistently until it is removed.

Malicious Mobile Code

Software with malicious intent that is transmitted from a remote host to a local host and then executed on the local host, typically without the user's explicit instruction. Popular languages for malicious mobile code include Java, ActiveX, JavaScript, and VBScript.

Network security measures

Network security measures are the security controls you add to your networks to protect confidentiality, integrity, and availability. These controls continue to evolve, but there is a lot of fundamental knowledge that readily available. It takes effort to keep attackers out of your network. Firewalls, proxies, and gateways work toward that end.

It is dangerous to assume that those devices will absolutely keep attackers out of your network. Hackers eventually find a way in. A well-known hacker, Kevin Mitnick, **claims 100% success** when launching penetration testing against companies that have hired him to test their network security.

There is always a way in. Security requires continued work to learn, evolve, and stay ahead of the hackers. It is also critical to have incident response plans and teams in place when hackers do get in.

Firewall

A firewall blocks or allows traffic to pass. The traffic allowed to pass through a firewall is specified in its configuration based on the type of traffic a business has and needs. The most important security best practice with a firewall is that it should block all traffic by default. It should then be configured to allow only specific traffic to known services. The configuration of the firewall is critical, so the firewall administrator's knowledge is crucial.

Firewalls operate at different layers within the International Standards Organisation Open System Interconnect (ISO OSI) model. Usually, anything called a firewall lives at layers 2-5. If the firewall is at layer 7, it is often referred to as a proxy or gateway. The exception is a web application firewall (WAF), which uses the word firewall and is at layer 7. A firewall analyses information found at the layer of the OSI model where it works.

Here are a few examples of how a firewall could operate at different layers:

- **Layer 2 – data link – it could make a block or forward decision based on the media access control (MAC) address on the frame.**
- **Layer 3 – network – it could make a block or forward decision based on the Internet Protocol (IP) address within the packet.**
- **Layer 4 – transport – it could make a block or forward decision based on the transmission control protocol (TCP) port number in the datagram.**
- **Layer 5 – session – it could make a block or forward decision based on the real-time protocol (RTP) information.**
- **Layer 7 – data – it could make a block or forward decision based on application or application service.**

A firewall is configured with a list of rules that are sometimes referred to as policies. The firewall uses this list of rules to determine what to do with traffic once it arrives at the firewall. The rules work from a top-down perspective.

The firewall compares the frame or packet it just received to the first rule in the list. If it matches the traffic type of that rule, it follows the instructions for that rule. A rule could say the traffic can pass, or that it should be blocked and discarded.

If the frame or packet does not match the first rule, the firewall compares it to the second and so on. If the traffic does not match one of the explicitly defined rules, the firewall will follow the final rule which should be to discard the traffic.

Proxy

A proxy firewall lives at layer 7 of the OSI model. When a proxy receives traffic, it processes the frame or packet up through the layers. For example, if the frame is stripped off at layer 2, the packet headers are removed at layer 3 and so on until only the data exists at layer 7.

The transport layer security (TLS) connection is terminated at layer 4, and the data is in clear text within the proxy from that point forward. The proxy then analyses the data being transmitted, which would have been impossible at lower levels because of the encryption. This enables the device to analyse a lot more data than a standard firewall. This usually takes more time or processing power than a firewall, but gives greater control over user traffic.

Gateway

The term gateway has different meanings depending on who you talk to. A gateway was traditionally a piece of hardware that sat between two networks. The average gateway today has a firewall

element in it. For example, Microsoft Azure has a WAF built into its gateway. So, a gateway is now debatably a type of firewall.

Intrusion detection & prevention systems

The next concern is to detect intrusions into a network using Intrusion detection systems (IDSs). These devices are passive. They watch network traffic go by and log suspicious traffic. An IDS could be on the network or the end device. Depending on where it is, it is called a network-based IDS (NIDS) or host-based IDS (HIDS).

A NIDS is usually connected to a tap or span port of a switch. This means that traffic is passed on to its destination without interference, and a copy goes to the span port of the NIDS for analysis. If it is a HIDS, it resides on the laptop, tablet, server, etc. Most HIDS do not analyse live traffic, but instead analyse traffic logs after the fact.

At some point, the manufacturers took these devices to the next level. If they can detect an attack, why not just trash suspicious frames or packets at the device instead of just reporting on it. This is how Intrusion prevention systems (IPS) came about. IPSs can also be network-based (NIPS) or host-based (HIPS).

This is a wonderful idea, but it comes with a downside. The IPS must know what is and is not good traffic. This can be done with signature files or it can learn.

Virtual private network (VPN)

The next concern to address is how to protect data, voice, or video that is transmitted anywhere someone might be able to eavesdrop. This includes within a corporate or home network and outside of those networks such as across the internet or on a service provider's network.

Encryption addresses this concern by making the data unreadable without the key. For data-in-transit, there are a few options for encryption. They are as follows:

- **Secure Socket Layer (SSL)/Transport Layer Security (TLS)**
- **Secure Shell (SSH)**
- **Internet Protocol Security (IPsec)**

SSL/TLS

SSL/TLS has been in use since 1995 to protect browser-based connections. Netscape invented SSL. Versions 2.0 and 3.0 were in use until the Internet Engineering Task Force (IETF) adopted and renamed it. This occurred in 1999 when America Online (AOL) bought Netscape. Now TLS 1.3 (RFC 8446) is the latest version. TLS is not only used for browser-based connections. It is also used for a user VPN connection to connect to the office.

SSL/TLS is a transport layer protocol that uses TCP port 443 when applied to browser connections.

SSH

SSH is an encryption method most commonly used for remote login capability. Network administrators use SSH to remotely login and administer network devices such as routers and switches. It is generally thought of as a replacement for Telnet, which is a layer 7 remote login protocol that is not encrypted, although it too can be used for VPN connections. SSH is specified in IETF RFC 4253. It uses TCP port 22.

IPsec

IPsec is a network layer protocol that provides encryption and integrity checking capability to any connection type. There are many different IETF RFC documents that specify the different parts of what is considered IPsec. RFC 6071 offers a roadmap showing how these documents relate to each other.

IPsec provides two security protocols: authentication header (AH) and encapsulating security payload (ESP).

- **AH is used to provide data origin authentication and integrity. An IPsec implementation does not have to support AH. AH encrypts the header of the IP packet.**
- **All IPsec implementations must support ESP, which offers data origin authentication, integrity and confidentiality. ESP encrypts the payload of the IP packet.**

Encryption is a security method in which information is encoded in such a way that only authorized user can read it. It uses encryption algorithm to generate ciphertext that can only be read if decrypted.

Types of Encryption

There are two types of encryptions schemes as listed below:

- Symmetric Key encryption
- Public Key encryption
- Decryption is a Cyber Security technique that makes it more difficult for hackers to intercept and read the information they're not allowed to do. It is transforming encrypted or encoded data or text back to its original plain format that people can easily read and understand from computer applications. This is the reverse of encryption, which requires coding data to make it unreadable for all, but only those with matching Decryption keys can read it.

A digital signature is **a mathematical technique used to validate the authenticity and integrity of a message, software or digital document**. ... Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages.A

Unit 5: IT Act. 2000 and Cyber Crimes [6 Marks, Class: 6]

IT Act 2000- Definitions of different terms, Digital signature, Electronic Governance, Attribution, Acknowledgement and Dispatch of Electronic Records, Regulation of Certifying Authorities, Digital Signatures Certificates, Duties of Subscribers, Penalties and Adjudication, Appellate Tribunal, Offences and Cyber-crimes.

1. Short title, extent, commencement and application.–(*1*) This Act may be called the Information Technology Act, 2000.

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.

(3) It shall come into force on such date[1] as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of thatprovision.

[2][(*4*) Nothing in this Act shall apply to documents or transactions specified in the First Schedule: Provided that the Central Government may, by notification in the Official Gazette, amend the First Schedule by way of addition or deletion of entries thereto.

(*5*) Every notification issued under sub-section (*4*) shall be laid before each House of Parliament.]

2. Definitions.–(*1*) In this Act, unless the context otherwise requires,–

(a) "access" with its grammatical variations and cognate expressions 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" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(c) "adjudicating officer" means an adjudicating officer appointed under sub-section (*1*) of section 46;

1. 17th October, 2000, *vide* notification No. G.S.R. 788 (E), dated 17th October, 2000, *see* Gazette of India, Extraordinary, Part II, sec. 3(*ii*).

2. Subs. by Act 10 of 2009, s. 3, for sub-section (*4*) (w.e.f. 27-10-2009).

(d) "affixing [1][electronic signature]" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

(e) "appropriate Government" means as respects any matter,–

(i) enumerated in List II of the Seventh Schedule to the Constitution;

(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution,

the State Government and in any other case, the Central Government;

(f) "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;

(g) "Certifying Authority" means a person who has been granted a licence to issue a [1][electronic signature] Certificate under section 24;

(h) "certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing [1][electronic signature] Certificates;

[2][(*ha*) "communication device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image;]

(i) "computer" means any electronic, magnetic, 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;

[3][(*j*) "computer network" means the inter-connection of one or more computers or computer systems or communication device through–

(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the inter-connection is continuously maintained;]

(k) "computer resource" means computer, computer system, computer network, data, computer data base or software;

(l) "computer system" means 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 programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communicationcontrol and other functions;

(m) "Controller" means the Controller of Certifying Authorities appointed under sub-section (*1*) of section 17;

(n) "Cyber Appellate Tribunal" means the Cyber [4]*** Appellate Tribunal established under sub-section (*1*) of section 48;

[2][(*na*) "cyber cafe" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public;

(*nb*) "cyber security means protecting information, equipment, devices, computer, computerresource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction;]

1. Subs. by Act 10 of 2009, s. 2, for "digital signature" (w.e.f. 27-10-2009).
2. Ins. by s. 4, *ibid*. (w.e.f. 27-10-2009).
3. Subs. by s. 4, *ibid*., for clause (*j*) (w.e.f. 27-10-2009).
4. The word "Regulations" omitted by s. 4, *ibid.* (w.e.f. 27-10-2009).

(o) "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised 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;

(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;

(q) "Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (*4*) of section 35;

(r) "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;

(s) "Electronic Gazette" means the Official Gazette published in the electronic form;

(t) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

[1][(*ta*) "electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature;

(*tb*) "Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate;]

(u) "function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

[1][(*ua*) Indian Computer Emergency Response Team" means an agency established under sub- section (*1*) of Section 70B;]

(v) "information" includes [2][data, message, text,] images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche;

[3][(*w*) "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;]

(x) "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 theprivate key;

(y) "law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be, Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (*a*) of clause (*1*) of article 357 of the Constitutionand includes rules, regulations, bye-laws and orders issued or made thereunder;

(z) "licence" means a licence granted to a Certifying Authority under section 24;

(*za*) "originator" means a person who sends, generates, stores or transmits any electronic messageor causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(*zb*) "prescribed" means prescribed by rules made under this Act;

(zc) "private key" means the key of a key pair used to create a digital signature;

(*zd*) "public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

1. Ins. by Act 10 of 2009 s. 4 (w.e.f. 27-10-2009).

2. Subs. by s. 4, *ibid.,* for "data, text", (w.e.f. 27-10-2009).

3. Subs. by s. 4, *ibid.,* for clause (*w*), (w.e.f. 27-10-2009).

(*ze*) "secure system" means computer hardware, software, and procedure that–

(a) are reasonably secure from unauthorised access and misuse;

(b) provide a reasonable level of reliability and correct operation;

(c) are reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures;

(*zf*) "security procedure" means the security procedure prescribed under section 16 by the Central Government;

(*zg*) "subscriber" means a person in whose name the [1][electronic signature] Certificate is issued; (*zh*)

"verify", in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions, means to determine whether–

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

(*2*) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

CHAPTER II

[2][DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE]

3. Authentication of electronic records.–(*1*) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronicrecord.

Explanation.–For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronicrecord as its input making it computationally infeasible–

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

[3]**[3A. Electronic signature.**–(*1*) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (*2*), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which–

(a) is considered reliable; and

(b) may be specified in the Second Schedule.

(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if–

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

1. Subs. by Act 10 of 2009, s. 2, for "digital signature" (w.e.f. 27-10-2009).
2. Subs. by s. 5, *ibid*., for the heading "DIGITAL SIGNATURE" (w.e.f. 27-10-2009).
3. Ins. by s. 6, *ibid.* (w.e.f. 27-10-2009).

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable;

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

(e) it fulfils such other conditions which may be prescribed.

(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.

(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule:

Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

(5) Every notification issued under sub-section (*4*) shall be laid before each House of Parliament.]

CHAPTER III

ELECTRONIC GOVERNANCE

4. Legal recognition of electronic records.–Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is–

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference.

5. Legal recognition of [1][electronic signatures].–Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of [1][electronic signature] affixed in such manner as may be prescribed by the Central Government.

Explanation.–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.

6. Use of electronic records and [1][electronic signatures] in Government and its agencies.–(*1*) Where any law provides for–

(a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner,

then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (*1*), by rules, prescribe–

(a) the manner and format in which such electronic records shall be filed, created or issued;

(b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (*a*).

1. Subs. by Act 10 of 2009, s. 2, for "digital signatures" (w.e.f. 27-10-2009).

[1][**6A. Delivery of services by service provider.**–(*1*) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorise, by order, any service provider to set up, maintain and upgrade the computerised facilities and perform such other services as it may specify, by notification in the Official Gazette.

Explanation.–For the purposes of this section, service provider so authorised includes any individual, private agency, private company, partnership firm, sole proprietor firm or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

(2) The appropriate Government may also authorise any service provider authorised under sub- section (*1*) to collect, retain and appropriate such service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

(3) Subject to the provisions of sub-section (*2*), the appropriate Government may authorise the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.

(4) The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section:

Provided that the appropriate Government may specify different scale of service charges for different types of services.]

7. Retention of electronic records.–(*1*) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if–

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

(*2*) Nothing in this section shall apply to any law that expressly provides for the retention ofdocuments, records or information in the form of electronic records.

[2][**7A. Audit of documents, etc., maintained in electronic form.–**Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall alsobe applicable for audit of documents, records or information processed and maintained in the electronic form.]

8. Publication of rule, regulation, etc., in Electronic Gazette.–Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that where any rule, regulation, order, by-law, notification or any other matter is publishedin the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

9. Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form.– Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should

1. Ins. by Act 10 of 2009 s. 7 (w.e.f. 27-10-2009).

2. Ins. by s. 8, *ibid.* (w.e.f. 27-10-2009).

accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

[Rules to be made by Central Government in respect of [electronic signature].–The Central Government may, for the purposes of this Act, by rules, prescribe–

(a) the type of [1][electronic signature];

(b) the manner and format in which the [1][electronic signature] shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the [1][electronic signature];

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to [1][electronic signatures].

[2]**[10A. Validity of contracts formed through electronic means.**–Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic records, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.]

CHAPTER IV

ATTRIBUTION, ACKNOWLEDGMENT AND DESPATCH OF ELECTRONIC RECORDS

11. Attribution of electronic records.–An electronic record shall be attributed to the originator–

(a) if it was sent by the originator himself;

(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(c) by an information system programmed by or on behalf of the originator to operate automatically.

12. Acknowledgment of receipt.–(*1*) Where the originator has not [3][stipulated] that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by–

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall he deemed to have been never sent by the originator.

(3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within thetime specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgement must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

13. Time and place of despatch and receipt of electronic record.–(*1*) Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

(2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an

1. Subs. by Act 10 of 2009, s. 2, for "digital signature" (w.e.f. 27-10-2009).
2. Ins. by s. 9, *ibid*. (w.e.f. 27-10-2009).
3. Subs. by s. 10, *ibid*., for "agreed with the addressee" (w.e.f. 27-10-2009).

electronic record shall be determined as follows, namely:–

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records,–

(i) receipt occurs at the time when the electronic record enters the designated computer resource; or

(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of sub-section (*2*) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (*3*).

(5) For the purposes of this section,–

(a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) "usual place of residence", in relation to a body corporate, means the place where it is registered.

CHAPTER V

SECURE ELECTRONIC RECORDS ANS SECURE [1][ELECTRONIC SIGNATURE]

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

[2]**[15. Secure electronic signature.–** An electronic signature shall be deemed to be a secure electronic signature if–

(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Explanation.–In case of digital signature, the "signature creation data" means the private key of the subscriber.

16. Security procedures and practices.–The Central Government may, for the purposes of sections 14 and 15, prescribe the security procedures and practices:

Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.]

CHAPTER VI

REGULATION OF CERTIFYING AUTHORITIES

17. Appointment of Controller and other officers.–(*1*) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers [3][, Assistant Controllers, other officers and employees] as it deems fit.

1. Subs. by Act 10 of 2009, s. 2, for "digital signatures" (w.e.f. 27-10-2009).
2. Subs. by s 11, *ibid.*, for sections 15 and 16 (w.e.f. 27-10-2009).
3. Subs. by s.47, *ibid.,* for "and Assistant Controllers" (w.e.f. 27-10-2009).

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) All powers and functions of the Deputy Controller and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers [1][,Assistant Controllers, other officers and employees] shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

18. Functions of Controller.–The Controller may perform all or any of the following functions, namely:–

(a) exercising supervision over the activities of the Certifying Authorities;

(b) certifying public keys of the Certifying Authorities;

(c) laying down the standards to be maintained by the Certifying Authorities;

(d) specifying the qualifications and experience which employees of the Certifying Authority should possess;

(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a [2][electronic signature] Certificate and the public key;

(g) specifying the form and content of a [2][electronic signature] Certificate and the key;

(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(m) laying down the duties of the Certifying Authorities;

(n) maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

19. Recognition of foreign Certifying Authorities.–(*1*) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under sub-section (*1*), the [2][electronic signature] Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (*1*) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

1. Subs. by Act 10 of 2009, s. 12, for "Assistant Controllers" (w.e.f. 27-10-2009).
2. Subs. by s. 2, *ibid.*, for "Digital Signature" (w.e.f. 27-10-2009).

20. [*Controller to act as repository.*] *Omitted by the Information Technology* (*Amendment*) *Act*, 2008 (10 *of* 2009), *s*. 13 (*w.e.f*. 27-10-2009).

[*Licence to issue [electronic signature] Certificates.*] Subject to the provisions of sub-section (*2*), any person may make an application, to the Controller, for a licence to issue [1][electronic signature] Certificates.

(2) No licence shall be issued under sub-section (*1*), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which arc necessary to issue [1][electronic signature] Certificates as may be prescribed by the Central Government.

(3) A licence granted under this section shall–

(a) be valid for such period as may be prescribed by the Central Government;

(b) not be transferable or heritable;

(c) be subject to such terms and conditions as may be specified by the regulations.

22. Application for licence.–(*1*) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a licence shall be accompanied by–

(a) a certification practice statement;

(b) a statement including the procedures with respect to identification of the applicant;

(c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

(d) such other documents, as may be prescribed by the Central Government.

23. Renewal of licence.–An application for renewal of a licence shall be–

(a) in such form;

(b) accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence.

24. Procedure for grant or rejection of licence.–The Controller may, on receipt of an application under sub-section (*1*) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application:

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

25. Suspension of licence.– (*1*) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has–

(a) made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;

(b) failed to comply with the terms and conditions subject to which the licence was granted;

[2][(*c*) failed to maintain the procedures and standards specified in section 30;]

(*d*) contravened any provisions of this Act, rule, regulation or order made thereunder,

revoke the licence:

Provided that no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (*1*), by order suspend such licence pending the completion of any enquiry ordered by him:

1. Subs. by Act 10 of 2009, s. 2, for "Digital Signature" (w.e.f. 27-10-2009).
2. Subs. by notification No. S.O. 1015(E) (w.e.f. 19-9-2002).

Provided that no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(*c*) No person whose licence has been suspended shall issue any [1][electronic signature] Certificate during such suspension.

26. Notice of suspension or revocation of licence.–(*1*) Where the licence of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the data base maintained by him.

(*2*) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories:

Provided that the data base containing the notice of such suspension or revocation, as the case maybe, shall be made available through a web site which shall be accessible round the clock:

Provided further that the Controller may, if he considers necessary, publicise the contents of data basein such electronic or other media, as he may consider appropriate.

27. Power to delegate.–The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

28. Power to investigate contraventions.–(*1*) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

(*2*) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 (43 of 1961), andshall exercise such powers, subject to such limitations laid down under that Act.

29. Access to computers and data.–(*1*) Without prejudice to the provisions of sub-section (*1*) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that [2][any contravention of the provisions of this Chapter] has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose ofsearching or causing a search to be made for obtaining any information or data contained in or availableto such computer system.

(*2*) For the purposes of sub-section (*1*), the Controller or any person authorised by him may, by order,direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

30. Certifying Authority to follow certain procedures.–Every Certifying Authority shall,–

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;

(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the [1][electronic signatures] are assured; [3]***

[4][(*ca*) be the repository of all electronic signature Certificates issued under this Act;

(*cb*) publish information regarding its practices, electronic signature Certificates and currentstatus of such certificates; and]

(d) observe such other standards as may be specified by regulations.

31. Certifying Authority to ensure compliance of the Act, etc.–Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made thereunder.

1. Subs. by Act 10 of 2009, s. 2, for "Digital Signature" (w.e.f. 27-10-2009).
2. Subs. by s. 14, *ibid.*, for "any contravention of the provisions of this Act, rules and regulations made thereunder" (w.e.f. 27-10-2009).
3. The word "and" omitted by s. 15, *ibid.* (w.e.f. 27-10-2009).
4. Ins. by s. 15, *ibid.* (w.e.f. 27-10-2009).

32. Display of licence.–Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

33. Surrender of licence.–(*1*) Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.

(*2*) Where any Certifying Authority fails to surrender a licence under sub-section (*1*), the person in whose favour a licence is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

34. Disclosure.–(*1*) Every Certifying Authority shall disclose in the manner specified by regulations–

(a) its [1][electronic signature] Certificate [2]***;

(b) any certification practice statement relevant thereto;

(c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a [1][electronic signature] Certificate, which that Authority has issued, or the Authority's ability to perform its services.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a [1][electronic signature] Certificate was granted, then, the Certifying Authority shall–

(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

CHAPTERVII

[1][ELECTRONIC SIGNATURE] CERTIFICATES

35. Certifying authority to issue [1][electronic signature] Certificate.–(*1*) Any person may make an application to the Certifying Authority for the issue of a [1][electronic signature] Certificate in such form as may be prescribed by the Central Government.

(2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority:

Provided that while prescribing fees under sub-section (*2*) different fees may be prescribed for different classes of applicants.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (*1*), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (*3*) and after making such enquiries as it may deem fit, grant the [1][electronic signature] Certificate or for reasons to be recorded in writing, reject the application:

[3]* * * * *

[4][Provided] that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

36. Representations upon issuance of Digital Signature Certificate.–A Certifying Authority while issuing a Digital Signature Certificate shall certify that–

(a) it has complied with the provisions of this Act and the rules and regulations made thereunder;

(b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

1. Subs. by Act 10 of 2009, s. 2, for "Digital Signature" (w.e.f. 27-10-2009).
2. Certain words omitted by s. 16, *ibid.* (w.e.f. 27-10-2009).
3. The first proviso omitted by s. 17, *ibid.* (w.e.f. 27-10-2009).
4. Subs. by s. 17, *ibid.*, for "Provided further" (w.e.f. 27-10-2009).

(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;

(*cb*) the public key to be listed in the certificate can be used to verify a digital signature affixed bythe private key held by the subscriber;]

(d) the subscriber's public key and private key constitute a functioning key pair;

(e) the information contained in the Digital Signature Certificate is accurate; and

(f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations in clauses (*a*) to (*d*).

37. Suspension of Digital Signature Certificate.–(*1*) Subject to the provisions of sub-section (*2*), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate,–

(a) on receipt of a request to that effect from–

(i) the subscriber listed in the Digital Signature Certificate; or

(ii) any person duly authorised to act on behalf of that subscriber;

(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.

(2) A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

(3) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

38. Revocation of Digital Signature Certificate.–(*1*) A Certifying Authority may revoke a Digital Signature Certificate issued by it–

(a) where the subscriber or any other person authorised by him makes a request to that effect; or

(b) upon the death of the subscriber; or

(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) Subject to the provisions of sub-section (*3*) and without prejudice to the provisions of sub-section (*1*), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that–

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

39. Notice of suspension or revocation.–(*1*) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

1. Ins. by Act 10 of 2009, s. 18 (w.e.f. 27-10-2009).

(*2*) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

40. 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, [1]*** the subscriber shall generate [2][that key] pair by applying the security procedure.

[3]**[40A. Duties of subscriber of Electronic Signature Certificate.–**In respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed.]

41. Acceptance of Digital Signature Certificate.–(*1*) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate–

(a) to one or more persons;

(b) in a repository; or

otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

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

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

42. Control of private key.–(*1*) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all stepsto prevent its disclosure [4]***.

(*2*) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

Explanation.–For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

CHAPTER IX

[5][PENALTIES, COMPENSATION AND ADJUDICATION]

43. [6]**[Penalty and compensation] for damage to computer, computer system, etc.**–If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,–

(a) accesses or secures access to such computer, computer system or computer network [7][or computer resource];

1. The word "then" omitted by notification No. S.O. 1015(E) (w.e.f. 19-9-2002).
2. Subs. *ibid.*, for "the key" (w.e.f. 19-9-2002).
3. Ins. by Act 10 of 2009, s. 19 (w.e.f. 27-10-2009).
4. The words "to a person not authorised to affix the digital signature of the subscriber" omitted by notification No. S.O.1015(E) (w.e.f. 19-9-2002).
5. Subs. by Act 10 of 2009, s. 20, for "PENALTIES AND ADJUDICATION" (w.e.f. 27-10-2009).
6. Subs. by s. 21, *ibid.*, for "Penalty" (w.e.f. 27-10-2009).

7. Ins. by s. 21, *ibid.* (w.e.f. 27-10-2009).

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

[1][(*i*) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(*j*) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;]

[2][he shall be liable to pay damages by way of compensation to the person so affected.]

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 usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer data-base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised 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.

[1][(*v*) "computer source code" means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form.]

[3]**[43A. Compensation for failure to protect data.**–Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

1. Ins. by Act 10 of 2009, s. 21 (w.e.f. 27-10-2009).

2. Subs. by s. 21, *ibid*., for certain words (w.e.f. 27-10-2009).
3. Ins. by s. 22, *ibid.* (w.e.f. 27-10-2009).

Explanation.–For the purposes of this section,–

(i) "body corporate" means any company and includes a firm or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.]

44. Penalty for failure to furnish information, return, etc.–If any person who is required under this Act or any rules or regulations made thereunder 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 therefor in the regulations fails to file return or furnish the same within the time specified therefor 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.

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

46. Power to adjudicate.–(*1*) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, [1][direction ororder made thereunder which renders him liable to pay penalty or compensation,] the Central Governmentshall, subject to the provisions of sub-section (*3*), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

[2][(*1A*) The adjudicating officer appointed under sub-section (*1*) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore:

Provided that the jurisdiction in respect of the claim for injury or damage exceeding rupees fivecrores shall vest with the competent court.]

(2) The adjudicating officer shall, after giving the person referred to in sub-section (*1*) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (*2*) of section 58, and–

1. Subs. by Act 10 of 2009, s. 23, for "direction or order made thereunder" (w.e.f. 27-10-2009).
2. Ins. by s. 23, *ibid*. (w.e.f. 27-10-2009).

(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code (45 of 1860);

(b) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1974);

[1][(*c*) shall be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code,1908 (5 of 1908).]

47. Factors to be taken into account by the adjudicating officer.–While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely:–

(a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(b) the amount of loss caused to any person as a result of the default;

(c) the repetitive nature of the default.

CHAPTER X

THE CYBER [2]*** APPELLATE TRIBUNAL

48. Establishment of Cyber Appellate Tribunal.–(*1*) The Central Government shall, bynotification, establish one or more appellate tribunals to be known as the Cyber [3]*** Appellate Tribunal.

(*2*) The Central Government shall also specify, in the notification referred to in sub-section (*1*), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

[4]**[49. Composition of Cyber Appellate Tribunal.–**(*1*) The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other Members, as the Central Government may, by notification in the Official Gazette, appoint:

Provided that the person appointed as the Presiding Officer of the Cyber Appellate Tribunal under theprovisions of this Act immediately before the commencement of the Information Technology (Amendment) Act, 2008 (10 of 2009) shall be deemed to have been appointed as the Chairperson of the said Cyber Appellate Tribunal under the provisions of this Act as amended by the Information Technology (Amendment) Act, 2008.

(2) The selection of Chairperson and Members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India.

(3) Subject to the provisions of this Act–

(a) the jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercised by the Benches thereof;

(b) a Bench may be constituted by the Chairperson of the Cyber Appellate Tribunal with one or two Members of such Tribunal as the Chairperson may deem fit.

(c) the Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Cyber Appellate Tribunal, by notification in the Official Gazette, specify;

(d) the Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction.

(4) Notwithstanding anything contained in sub-section (*3*), the Chairperson of the Cyber Appellate Tribunal may transfer a Member of such Tribunal from one Bench to another Bench.

(5) If at any stage of the hearing of any case or matter it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit.

1. Ins. by Act 10 of 2009, s. 23 (w.e.f. 27-10-2009).

2. The word "REGULATIONS" omitted by s. 24, *ibid.* (w.e.f. 27-10-2009).
3. The word "Regulations" omitted by s. 25, *ibid.* (w.e.f. 27-10-2009).
4. Subs. by s. 26, *ibid.*, for sections 49 to 52 (w.e.f. 27-10-2009).

50. Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal.–

(1) A person shall not be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a Judge of a High Court.

(2) The Members of the Cyber Appellate Tribunal, except the Judicial Member to be appointed under sub-section (*3*), shall be appointed by the Central Government from amongst persons, having special knowledge of, and professional experience in, information technology, telecommunication, industry, management or consumer affairs:

Provided that a person shall not be appointed as a Member, unless he is, or has been, in the service of the Central Government or a State Government, and has held the post of Additional Secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than one year or Joint Secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than seven years.

(3) The Judicial Members of the Cyber Appellate Tribunal shall be appointed by the Central Government from amongst persons who is or has been a member of the Indian Legal Service and has held the post of Additional Secretary for a period of not less than one year or Grade I post of that Service for a period of not less than five years.

51. Term of office, conditions of service, etc., of Chairperson and Members.–(*1*) The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

(2) Before appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member.

(3) An officer of the Central Government or State Government on his selection as the Chairperson or Member of the Cyber Appellate Tribunal, as the case may be, shall have to retire from service before joining as such Chairperson or Member.

52. Salary, allowances and other terms and conditions of service of Chairperson and Members.–The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Chairperson or a Member of the Cyber Appellate Tribunal shall be such as may be prescribed.

52A. Powers of superintendence, direction, etc.–The Chairperson of the Cyber Appellate Tribunal shall have powers of general superintendence and directions in the conduct of the affairs of that Tribunal and he shall, in addition to presiding over the meetings of the Tribunal, exercise and discharge such powers and functions of the Tribunal as may be prescribed.

52B. Distribution of business among Benches.–Where Benches are constituted, the Chairperson of the Cyber Appellate Tribunal may, by order, distribute the business of that Tribunal amongst the Benches and also the matters to be dealt with by each Bench.

52C. Power of Chairperson to transfer cases.–On the application of any of the parties and after notice to the parties, and after hearing such of them as he may deem proper to be heard, or *suo motu* without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one Bench, for disposal to any other Bench.

52D. Decision by majority.–If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the Cyber Appellate Tribunal who shall hear the point or points himself and such point or points shall be decided according to the opinion of the majority of the Members who have heard the case, including those who first heard it.]

53. Filling up of vacancies.–If, for reason other than temporary absence, any vacancy occurs in the office of the [1][Chairperson or Member, as the case may be,] of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

1. Subs. by Act 10 of 2009, s. 27, for "Presiding Officer" (w.e.f. 27-10-2009).

54. Resignation and removal.–(*1*) The [1][Chairperson or the Member] of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

Provided that the [1][Chairperson or the Member] shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his officeor until the expiry of his term of office, whichever is the earliest.

(2) The [1][Chairperson or the Member] of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehavior or incapacity after an inquiry made by a Judge of the Supreme Court in which the [1][Chairperson or the Member] concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

(3) The Central Government may, by rules, regulate the procedure for the investigation of misbehavior or incapacity of the aforesaid [1][Chairperson or the Member].

55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings.–No order of the Central Government appointing any person as the [2][Chairperson or the Member] of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

56. Staff of the Cyber Appellate Tribunal.–(*1*) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the [3][Chairperson].

(3) The salaries, allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

57. Appeal to Cyber Appellate Tribunal.–(*1*) Save as provided in sub-section (*2*), any person aggrieved by an order made by controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (*1*) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:

Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said periodof forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (*1*), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (*1*) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

58. Procedure and powers of the Cyber Appellate Tribunal.–(*1*) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place atwhich it shall have its sittings.

1. Subs. by Act 10 of 2009, s. 28, for "Presiding Officer" (w.e.f. 27-10-2009).
2. Subs. by s. 29, *ibid.*, for "Presiding Officer" (w.e.f. 27-10-2009).
3. Subs. by s. 30, *ibid.*, for "Presiding Officer" (w.e.f. 27-10-2009).

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:–

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses or documents;

(e) reviewing its decisions;

(f) dismissing an application for default or deciding it *ex parte*;

(g) any other matter which may be prescribed.

(3) Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code (45 of 1860) and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).

59. Right to legal representation.–The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

60. Limitation.–The provisions of the Limitation Act, 1963 (36 of 1963), shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

61. Civil court not to have jurisdiction.–No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

62. Appeal to High Court.–Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order:

Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceedingsixty days.

63. Compounding of contraventions.–(*1*) Any contravention under this [1][Act] may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorised by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:

Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which maybe imposed under this Act for the contravention so compounded.

(2) Nothing in sub-section (*1*) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Explanation.–For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

(3) Where any contravention has been compounded under sub-section (*1*), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

1. Subs. by notification No. S.O. 1015(E) (w.e.f. 19-9-2002).

64. Recovery of [1][penalty].–A [2][penalty imposed or compensation awarded] under this Act, if it is not paid, shall he recovered as an arrear of land revenue and the licence or the [3][electronic signature] Certificate, as the case may be, shall be suspended till the penalty is paid.

CHAPTER XI

OFFENCES

65. Tampering with computer source documents.–Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.–For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

[4][**66. Computer related offences.**–If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Explanation.–For the purposes of this section,–

(a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860);

(b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).

66A. Punishment for sending offensive messages through communication service, etc.–Anyperson who sends, by means of a computer resource or a communication device,–

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation.–For the purpose of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, images, audio, video and any other electronic record, which may be transmitted with the message.

66B. Punishment for dishonestly receiving stolen computer resource or communication device.–Whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

66C. Punishment for identity theft.–Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

1. Subs. by Act 10 of 2009, s. 31, for "penalty" (w.e.f. 27-10-2009).

2. Subs. by s. 31, *ibid*., for "penalty imposed" (w.e.f. 27-10-2009).
3. Subs. by s. 2, *ibid*., for "Digital Signature" (w.e.f. 27-10-2009).
4. Subs. by s. 32, *ibid*., for sections 66 and 67 (w.e.f. 27-10-2009).

66D. Punishment for cheating by personation by using computer resource.–Whoever, by means of any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

66E. Punishment for violation of privacy.–Whoever, intentionally or knowingly captures, publishesor transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three yearsor with fine not exceeding two lakh rupees, or with both.

Explanation.–For the purposes of this section–

(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "private area" means the naked or undergarment clad genitals, public area, buttocks or female breast:

(d) "publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that–

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

66F. Punishment for cyber terrorism.–(*1*) Whoever,–

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by–

(i) denying or cause the denial of access to any person authorised to access computerresource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,

commits the offence of cyber terrorism.

(*2*) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

67. Punishment for publishing or transmitting obscene material in electronic form.–Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter

contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.–Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

67B. Punishment for publishing or transmitting of material depicting children in sexuallyexplicit act, etc., in electronic form.–Whoever,–

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extendto five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form–

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for *bonafide* heritage or religious purposes.

Explanation–For the purposes of this section, "children" means a person who has not completed the age of 18 years.

67C. Preservation and retention of information by intermediaries.–(*1*) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and formatas the Central Government may prescribe.

(*2*) any intermediary who intentionally or knowingly contravenes the provisions of sub-section (*1*) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.]

68. Power of Controller to give directions.–(*1*) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.

[1][(*2*) Any person who intentionally or knowingly fails to comply with any order under sub-section (*1*) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or with both.]

1. Subs. by Act 10 of 2009, s. 33, for sub-section (*2*) (w.e.f. 27-10-2009).

[1][69. **Power to issue directions for interception or monitoring or decryption of any information through any computer resource.**–(*1*) Where the Central Government or a State Government or any ofits officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (*2*), for reasons to be recordedin writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (*1*), extend all facilities and technical assistance to–

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, monitor, or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (*3*) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

69A. Power to issue directions for blocking for public access of any information through any computer resource.–(*1*) Where the Central Government or any of its officers specially authorised by it inthis behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to theprovisions of sub-section (*2*), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (*1*) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security.–(*1*) The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The intermediary or any person in-charge or the computer resource shall, when called upon by the agency which has been authorised under sub-section (*1*), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (*2*) shall be punished with an imprisonment for a term which any extend to three years and shall also be liable to fine.

Explanation.–For the purposes of this section,–

(i) "computer contaminant" shall have the meaning assigned to it in section 43;

1. Subs. by Act 10 of 2009, s. 34, for section 69 (w.e.f. 27-10-2009).

(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data, size, duration or type of underlying service and any other information.]

70. Protected system.–[1][(*1*) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation.–For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.]

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (*1*).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

[2][(*4*) The Central Government shall prescribe the information security practices and procedures for such protected system.]

[3]**[70A. National nodal agency.**–(*1*) The Central Government may, by notification published in the Official Gazette, designate any organisation of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.

(2) The national nodal agency designated under sub-section (*1*) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.

(3) The manner of performing functions and duties of the agency referred to in sub-section (*1*) shall be such as may be prescribed.

70B. Indian Computer Emergency Response Team to serve as national agency for incident response.–(*1*) The Central Government shall, by notification in the Official Gazette, appoint an agency of the Government to be called the Indian Computer Emergency Response Team.

(2) The Central Government shall provide the agency referred to in sub-section (*1*) with a Director General and such other officers and employees as may be prescribed.

(3) The salary and allowances and terms and conditions of the Director-General and other officers and employees shall be such as may be prescribed.

(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security,–

(a) collection, analysis and dissemination of information on cyber incidents;

(b) forecast and alerts of cyber security incidents;

(c) emergency measures for handling cyber security incidents;

(d) coordination of cyber incidents response activities;

(e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, preventation, response and reporting of cyber incidents;

(f) such other functions relating to cyber security as may be prescribed.

(5) The manner of performing functions and duties of the agency referred to in sub-section (*1*) shall be such as may be prescribed.

(6) For carrying out the provisions of sub-section (*4*), the agency referred to in sub-section (*1*) may call for information and give direction to the service providers, intermediaries, data centres, body corporate and any other person.

1. Subs. by Act 10 of 2009, s. 35, for sub-section (*1*) (w.e.f. 27-10-2009).

2. Ins. by s. 35, *ibid.* (w.e.f. 27-10-2009).

3. Ins. by s. 36, *ibid.* (w.e.f. 27-10-2009).

(7) Any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (*6*), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(8) No court shall take cognizance of any offence under this section, except on a complaint made by an officer authorised in this behalf by the agency referred to in sub-section (*1*).]

71. Penalty for misrepresentation.–Whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any licence or [1][electronic signature] Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

72. Penalty for Breach of confidentiality and privacy.–Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

[2][**72A. Punishment for disclosure of information in breach of lawful contract.**–Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likelyto cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.]

73. Penalty for publishing [1][electronic signature] Certificate false in certain particulars.–(*1*) No person shall publish a [1][electronic signature] Certificate or otherwise make it available to any other person with the knowledge that–

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying a [1][electronic signature] created prior to such suspension or revocation.

(*2*) Any person who contravenes the provisions of sub-section (*1*) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

74. Publication for fraudulent purpose.–Whoever knowingly creates, publishes or otherwise makes available a [1][electronic signature] Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

75. Act to apply for offence or contravention committed outside India.–(*1*) Subject to the provisions of sub-section (*2*), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(*2*) For the purposes of sub-section (*1*), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

76. Confiscation.–Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation:

1. Subs. by Act 10 of 2009, s. 2, for "Digital Signature" (w.e.f. 27-10-2009).
2. Ins. by s. 37, *ibid.* (w.e.f. 27-10-2009).

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

[1][**77. Compensation, penalties or confiscation not to interfere with other punishment.**–No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

77A. Compounding of offences.–A court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years hasbeen provided, under this Act:

Provided that the court shall not compound such offence where the accused is, by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind:

Provided further that the court shall not compound any offence where such offence affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

(*2*) The person accused of an offence under this Act may file an application for compounding in the court in which offence is pending for trial and the provisions of sections 265B and 265C of the Code of Criminal Procedure, 1973 (2 of 1974) shall apply.

77B. Offences with three years imprisonment to be bailable.–Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.]

78. Power to investigate offences.–Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of [2][Inspector] shall investigate any offence under this Act.

[3][CHAPTER XII

INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

79. Exemption from liability of intermediary in certain cases.–(*1*) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (*2*) and (*3*), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (*1*) shall apply if–

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) the intermediary does not–

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

1. Subs. by Act 10 of 2009, s. 38, for section 77 (w.e.f. 27-10-2009).

2. Subs. by s. 39, *ibid.*, for "Deputy Superintendent of Police" (w.e.f. 27-10-2009).
3. Subs. by s. 40, *ibid.*, for Chapter XII (w.e.f. 27-10-2009).

(3) The provisions of sub-section (*1*) shall not apply if–

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation.–For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

CHAPTER XIIA EXAMINER OF ELECTRONIC EVIDENCE

79A. Central Government to notify Examiner of Electronic Evidence.–The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation.–For the purposes of this section, "electronic form evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.]

CHAPTER XIII

MISCELLANEOUS

80. Power of police officer and other officers to enter, search, etc.–(*1*) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of a [1][Inspector], or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of beingabout to commit any offence under this Act.

Explanation.–For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (*1*) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 (2 of 1974) shall, subject to theprovisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

81. Act to have overriding effect.–The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

[2][Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 (14 of 1957) or the Patents Act, 1970 (39 of 1970).]

[3]**[81A. Application of the Act to electronic cheque and truncated cheque.–**(*1*) The provisions of this Act, for the time being in force, shall apply to, or in relation to, electronic cheques and the truncated cheques subject to such modifications and amendments as may be necessary for carrying out the purposesof the Negotiable Instruments Act, 1881 (26 of 1881) by the Central Government, in consultation with theReserve Bank of India, by notification in the Official Gazette.

(*2*) Every notification made by the Central Government under sub-section (*1*) shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty

1. Subs. by Act 10 of 2009, s. 41, for "Deputy Superintendent of Police" (w.e.f. 27-10-2009).
2. Ins. by s. 42, *ibid.* (w.e.f. 27-10-2009).
3. Ins. by Act 55 of 2002, s. 13 (w.e.f. 26-2-2003).

days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the notification or both Houses agree that the notification should not be made, the notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that notification.

Explanation.–For the purposes of this Act, the expressions "electronic cheque" and "truncated cheque" shall have the same meaning as assigned to them in section 6 of the Negotiable Instruments Act, 1881 (26 of 1881).]

82. [1][Chairperson, Members, officers and employees to be public servants].–The [2][Chairperson, Members] and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code (45 of 1860).

83. Power to give directions.–The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made thereunder.

84. Protection of action taken in good faith.–No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the [3][Chairperson, Members], adjudicating officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made thereunder.

[4][**84A. Modes or methods for encryption.**–The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption.

84B. Punishment for abetment of offences.–Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for thepunishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation.–An act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

84C. Punishment for attempt to commit offences.–Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both.]

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

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

(*2*) Notwithstanding anything contained in sub-section (*1*), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company,

1. Subs. by Act 10 of 2009, s. 43, for the marginal heading (w.e.f. 27-10-2009).
2. Subs. by s. 43, *ibid.*, for "Presiding Officer" (w.e.f. 27-10-2009).
3. Subs. by s. 44, *ibid.*, for "Presiding Officer" (w.e.f. 27-10-2009).
4. Ins. by s. 45, *ibid.* (w.e.f. 27-10-2009).

such director, manager, secretary or other officer shall also be deemed to be guilty of the contraventionand shall be liable to be proceeded against and punished accordingly.

Explanation.–For the purposes of this section,–

(i) "company" means any body corporate and includes a firm or other association of individuals; and

(ii) "director", in relation to a firm, means a partner in the firm.

86. Removal of difficulties.–(*1*) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty:

Provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this Act.

(*2*) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

87. Power of Central Government to make rules.–(*1*) The Central Government may, by notification in the Official Gazette and in the Electronic Gazette, make rules to carry out the provisions of this Act.

(*2*) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:–

[1][(*a*) the conditions for considering reliability of electronic signature or electronic authentication technique under sub-section (*2*) of section 3A;

(*aa*) the procedure for ascertaining electronic signature or authentication under sub-section (*3*) ofsection 3A;

(*ab*) the manner in which any information or matter may be authenticated by means of electronic signature under section 5;]

(b) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (*1*) of section 6;

(c) the manner and format in which electronic records shall be filed, or issued and the method of payment under sub-section (*2*) of section 6;

[2][(*ca*) the manner in which the authorised service provider may collect, retain and appropriateservice charges under sub-section (*2*) of section 6A;]

(d) the matters relating to the type of [3][electronic signature], manner and format in which it may be affixed under section 10;

[4][(*e*) the manner of storing and affixing electronic signature creation data under section 15;(*ea*)

the security procedures and practices under section 16;]

(*f*) the qualifications, experience and terms and conditions of service of Controller, DeputyControllers [5][, Assistant Controllers, other officers and employees] under section 17;

[6]* * * * *

(h) the requirements which an applicant must fulfil under sub-section (*2*) of section 21;

(i) the period of validity of licence granted under clause (*a*) of sub-section (*3*) of section 21;

(j) the form in which an application for licence may be made under sub-section (*1*) of section 22;

1. Subs. by Act 10 of 2009, s. 46, for clause (*a*) (w.e.f. 27-10-2009).

2. Ins. by s. 46, *ibid.* (w.e.f. 27-10-2009).

3. Subs. by s. 5, *ibid.,* for "digital signature" (w.e.f. 27-10-2009).

4. Subs. by s. 46, *ibid.,* for clause (*e*) (w.e.f. 27-10-2009).

5. Subs. by s. 46, *ibid.*, for "and Assistant Controllers" (w.e.f. 27-10-2009).

6. Clause (*g*) omitted by s. 46, *ibid.* (w.e.f. 27-10-2009).

(k) the amount of fees payable under clause (*c*) of sub-section (*2*) of section 22;

(l) such other documents which shall accompany an application for licence under clause (*d*) of

(m) the form and the fee for renewal of a licence and the fee payable thereof under section 23;

[1][(*ma*) the form of application and fee for issue of Electronic Signature Certificate undersection 35;]

(n) the form in which application for issue of a [2][electronic signature] Certificate may be made under sub-section (*1*) of section 35;

(o) the fee to be paid to the Certifying Authority for issue of a [2][electronic signature] Certificate under sub-section (*2*) of section 35;

[1][(*oa*) the duties of subscribers under section 40A;

(*ob*) the reasonable security practices and procedures and sensitive personal data or informationunder section 43A;]

(p) the manner in which the adjudicating officer shall hold inquiry under sub-section (*1*) of section 46;

(q) the qualification and experience which the adjudicating officer shall possess under sub-section (*3*) of section 46;

(r) the salary, allowances and the other terms and conditions of service of the [3][Chairperson and Members] under section 52;

(s) the procedure for investigation of misbehaviour or incapacity of the [3][Chairperson and Members] under sub-section (*3*) of section 54;

(t) the salary and allowances and other conditions of service of other officers and employees under sub-section (*3*) of section 56;

(u) the form in which appeal may be filed and the fee thereof under sub-section (*3*) of section 57;

(v) any other power of a civil court required to be prescribed under clause (*g*) of sub-section (*2*) of section 58; and

[4][(*w*) the powers and functions of the Chairperson of the Cyber Appellate Tribunal undersection 52A;

(x) the information, duration, manner and form of such information to be retained and preserved under section 67C;

(y) the procedures and safeguards for interception, monitoring or decryption under sub-section (*2*) of section 69A;

(z) the procedures and safeguards for blocking for access by the public under sub-section (*3*) of section 69 B;

(*za*) the procedure and safeguards for monitoring and collecting traffic data or information undersub-section (*3*) of section 69B;

(*zb*) the information security practices and procedures for protected system under section 70;

(*zc*) manner of performing functions and duties of the agency under sub-section (*3*) ofsection 70 A;

(*zd*) the officers and employees under sub-section (*2*) of section 70B;

(*ze*) salaries and allowances and terms and conditions of service of the Director General and otherofficers and employees under sub-section (*3*) of section 70B;

1. Ins. by Act 10 of 2009, s. 46 (w.e.f. 27-10-2009).

2. Subs. by, s. 5, for "digital signature" (w.e.f. 27-10-2009).
3. Subs. by s. 46, *ibid.*, for "Presiding Officer" (w.e.f. 27-10-2009).
4. Subs. by s. 46, *ibid.*, for clause (*w*) (w.e.f. 27-10-2009).

(*zf*) the manner in which the functions and duties of agency shall be performed under sub-section (*5*) of section 70B;

(*zg*) the manner of performing functions and duties under sub-section (*2*) of section 70B;

(*zh*) the guidelines to be observed by the intermediaries under sub-section (*2*) of section 79; [1][(*zi*) the modes or methods for encryption under section 84 A.]

(*3*) [1][Every notification made by the Central Government under sub-section (*1*) of section 70A and every rule made by it] shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or thesuccessive sessions aforesaid, both Houses agree in making any modification in [2]*** the rule or both Houses agree that [2]*** the rule should not be made, [2]*** the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that notification orrule.

88. Constitution of Advisory Committee.–(*1*) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.

(2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit.

(3) The Cyber Regulations Advisory Committee shall advise–

(a) the Central Government either generally as regards any rules or for any other purposeconnected with this Act;

(b) the Controller in framing the regulations under this Act.

(4) There shall be paid to the non-official members of such Committee such travelling and other allowances as the Central Government may fix.

89. Power of Controller to make regulations.–(*1*) The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made thereunder to carry out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:–

(a) the particulars relating to maintenance of data base containing the disclosure record of every Certifying Authority under clause [3][(*n*)] of section 18;

(b) the conditions and restrictions subject to which the Controller may recognise any foreign Certifying Authority under sub-section (*1*) of section 19;

(c) the terms and conditions subject to which a licence may be granted under clause (*c*) of sub-section (*3*) of section 21;

(d) other standards to be observed by a Certifying Authority under clause (*d*) of section 30;

(e) the manner in which the Certifying Authority shall disclose the matters specified in sub-section (*1*) of section 34;

(f) the particulars of statement which shall accompany an application under sub-section (*3*) of section 35.

(g) the manner by which the subscriber shall communicate the compromise of private key to the Certifying Authority under sub-section (*2*) of section 42.

1. Subs. by Act 10 of 2009, s. 46, for certain words, brackets, letter and figures (w.e.f. 27-10-2009).
2. The words "the notification or" omitted by s. 46, *ibid.* (w.e.f. 27-10-2009).
3. Subs. by notification No. S.O. 1015(E), for "(*m*)" (w.e.f. 19-9-2002).

(3) Every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the aforesaid successive sessions, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously doneunder that regulation.

90. Power of State Government to make rules.–(*1*) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:–

(a) the electronic form in which filing, issue, grant, receipt or payment shall be effected under sub-section (*1*) of section 6;

(b) for matters specified in sub-section (*2*) of section 6;

[1]* * * * *

(3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the Stale Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

91. [*Amendment of Act* 45 *of* 1860**.]** *Omitted by the Information Technology* (*Amendment*) *Act*, 2008 (10 of 2009), *s.* 48 (*w.e.f.* 27-10-2009).

92. [*Amendment of Act* 1 *of* 1872.] *Omitted by s.* 48, *ibid.* (*w.e.f.* 27-10-2009).

93. [*Amendment of Act* 18 *of* 1891.] *Omitted by s.* 48, *ibid.* (*w.e.f.* 27-10-2009).

94. [*Amendment of Act* 2 *of* 1934.] *Omitted by s.* 48, *ibid.* (*w.e.f.* 27-10-2009).

1. Clause (*c*) omitted by Act 10 of 2009, s. 47 (w.e.f. 27-10-2009).