Contents

This chapter introduces the topic Cyber law and Ethics. After completion of this chapter you will

- Understand the terms Moral, Ethics and Law
- Understand the need for Ethics Culture, Ethics for computer users, Computer professionals, Business Information Service
- Be able to define the code of ethics and ethics guidelines
- Introduced to cyber laws
- Understand the Information Technology Act of India, 2000
- Understand the Definitions of the terms like digital Signature, Electronic Records – Attribution, Acknowledgement and Dispatch
- Be familiar with the ten Commandments of Computing
- Be understanding the need of Security, Privacy and Control and the methods to achieve it.
- Be able to understand the purpose and use of Intellectual Property Rights

Introduction :

Computers and their use is a day to day activity of all the students, professionals, teachers, universities, banks, supermarkets, in the entertainment field, in medical profession and also in higher education. The use of this weapon is spreading very widely in all parts of our society. As every weapon has two ways of operation. One is good and essential and the other is bad and not essential. Many times, whenever a new weapon is invented, many people uses it unknowingly for the wrong purpose. So to aware them and to make the proper use of the power of the newly invented weapon, laws are to be formulated and should be implemented. This chapter introduces the cyber law and many terms involved in it.

Let us begin our discussion by defining the term **'Cyber Crime'**. There are two basic definitions of cyber crime. (a) One definition says that 'cyber crime' consists of only those offences provided in the Information technology Act, 2000. As per this definition, cyber crimes would mainly be restricted to tampering with the computer source code, hacking and cyber pornography. Cyber fraud, defamation, harassment, e – mail abuse and IPR thefts, would not classify as cyber crimes. (b) In second definition, 'cyber crime' is said to be an act of commission or omission with the internet, committed on the internet or through the internet or with the help of the internet or connected with the internet, whether directly or indirectly, which is prohibited by the law and for which punishment, momentary and / or corporal is provided.

According to these definitions, the IT Act, 2000 provides punishments for only certain cyber offences and is not applicable to all the cyber crimes. For example, suppose a person threatens any other person with causing death or serious hurt. Then he will be liable for the offence of criminal intimidation under section 506 of the Indian Penal Code, 1860. But he will not be liable for the offence under the IT Act, 2000. But this act would be classified as the cyber crime. Another example which can be seen is that, suppose a person cheats another person using the Internet. Then he shall be liable for cheating under section 420 of IPC but not under the IT Act, 2000. But his act would be commonly called as a cyber fraud but it can not be classified as the cyber crime.

Cyber crimes can be classified as follows.

(a) Old crimes, committed on or through the new medium of the Internet. for example, cheating, fraud, misappropriation, defamation, pornography, threats, etc. committed on the Internet or through the Internet or with the help of internet, would fall under this category. These crimes are old but their place of operation is new, i.e. the Internet. The Internet with its speed and global access has made these crimes much easier, efficient, risk free, cheap and profitable to commit. These can be called as crimes "on" the Internet.

(b) New crimes created with the Internet itself, such as hacking, planting viruses and IPR thefts. These can be called as the crimes "of" the Internet.

(c) New crimes used for commission of old crimes. For instance, where hacking is committed to carry out cyber frauds.

Computer crimes have also been classified by the nature of the usage of the computer.

(a) Proper computer crimes such as hacking where a computer and network are essential for the commission of the offence.

(b) Computer assisted crimes such as cyber pornography where the medium of the internet is used.

(c) Crimes where the computer is only incidental for commission such as cyber fraud.

Though the IT Act, 2000 specifically defines and punishes only a few cyber crimes, it recognizes that there are other cyber crimes of cyberspace which are provided in the Indian Penal Code, 1860. It was perceived by out legislators that many of the offences in IPC ceased to apply cyberspace because the definition of "document" did not include within its domain "electronic records". Hence it was found necessary by our law makers to modify the various provisions of IPC by specifically making "electronic records" a part of thereof.

In short, cyber crime is the most dangerous of all crimes because of the magnitude of the loss that it is causing today and its potential, ease with which it is committed; its invisibility and the disregard for geographical boundaries; the difficulty in investigation, collection of evidence and the successful examination of the cyber criminal; and the costs of dealing with cyber crime by law enforcement and protective technology. Once the Internet becomes an integral part of the daily life of even the common man, which is not very far away, cyber crime, if not checked, would be destructive to civilization itself.

Therefore the growth of the Internet should be directly linked with the growth of protective technology and other means of checking and controlling the cyber crimes. It will be in the interest of the society, for the Internet and e – commerce to grow slowly but steadily, rather than grow into a bubble only to burst. Terrorism has already become a global phenomenon. It needs to be remembered that the development of technology is equal for all including the terrorist. In this millennium, the terrorist will not need to board an aircraft to hijack it. He will only need to break into and assume control over the computer systems which manage the air travel.

So as to effectively check cyber criminality, besides deterrent laws and protective technology, certain fundamental changes are necessary in the functioning of the Internet. Proper and easy identification of netizens is absolutely necessary for the effective control on cyber crimes. It should be realized that the cyber crime is a problem which influences the entire world and not just a few countries. Efforts are being made internationally to form a global strategy to counter cyber crime.

Copyright

Copyright is an intellectual property right attached to original works in which the right subsists with it. Copyright is a form of protection provided by the law to the author's of original works of authorship including literacy, dramatic, musical, and artistic and certain other intellectual works. This protection is available to both published and unpublished works. Copyright law is useful for authorship determination, duration of protection and requirements for transfers of rights to others.

Security

Security is an organizational concern, business needs safeguards that protect computer systems and data from damage or unlawful use.

Privacy

Privacy is an individual concern, people need assurance that their personal information such as employment and credit history will be used properly.

Control

Controls are policies, procedures, tools and techniques designed to prevent errors in data, software and systems. Access privileges, input authorization, data validations, documentation, fire alarms, training, effective communications are certain controls.

Digital Signature

A digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure. To secure data on the internet digital signature is used. It is unique to the subscriber who is affixing it so it is used to identifying such subscribers. It is linked to the electronic record to which it relates in such a manner that if the electronic record was altered, the digital signature would be invalidated. Digital

signature uses encryption tool to send the message that is unreadable until expected recipient uses their private key to decrypt the message.

Public Key and Private Key

Public key means the key of a key pair used to verify a digital signature and listed in digital signature certificate. Private key means the key of a key pair used to create a digital signature.

Cyber Law

Cyber law refers to all the legal and regulatory aspects of internet and the World Wide Web. Cyber space is governed by a system of law and regulations called cyber law. Cyber law is needed because of the following reasons (a) Today millions of people are using the internet all over the world. Because of global communications, internet is misused for criminal activities which require regulation. Today many disturbing and unethical things are happening in the cyber space which are known as cyber crimes. People with intelligence and having bad intensions are misusing the aspect of internet.

Software Piracy

Software piracy is unauthorized duplication, distribution and use of computer software. Copying of the software without purchasing it is known as pirating the software and such a copy of software is known as pirated software. The use of pirated software is the violation of the IT act 2000 as well as it is unethical. Software pirates have known to manipulate internet auction sites to reach hundreds of unwitting consumers everyday at little cost. With the growth of the internet, however, software pirates rapidly understood to take advantage of the wide audience available on global networks. For making more copies of the software than the license copy. Or installing licensed software for one computer and copied that software on other machines. To prevent the software piracy some companies set up software locks and limits the number of installations while some use hardware locks so that the software can not be used by unauthorized person illegally.

Ethics for computer users

All computer users have the responsibility to use computer system with an effective, efficient, ethical and lawful manner. Computer users must be responsible towards the profession, organization and society. They should prevent an unauthorized duplication, distribution and use of computer software. Many people, when not authorized, try to access information and will be held responsible for unauthorized access. In information technology, everyone has right to access the data but up to a limited extent and form authentic source only.

Need for Ethics culture

The use of computers is spreading everywhere. Millions of computer systems are networked together and thus the vast amount of information is now handled together at a time. The culture of ethics needs to be promoted in order to get appropriate use of computer and information transfer. Use of ethics also safeguards the privacy of the user and gives many more advantages. In information technology hacking of data, virus infection, loss of data, unauthorized access, unauthorized use of passwords are the major threats. Ethics culture is necessary in order to overcome these threats and proceed towards the safety of the information, data and hence that of the society.

Moral

Moral refers to the generally accepted standards of deciding right and wrong things in a society. It also refers to the standards of right conduct and the judgment of particular actions. Moral theory is a set of moral principles which systematically links moral beliefs to one another.

Ethics

Ethics is the determination of what is wrong and what is right and then doing the right things. It includes the fundamental, traditional basic rules which we follow in our life. Ethics states that allow each person to take free and autonomous choice which is unaffected by the surroundings. Ethics gives justice to each person according to its individual efforts.

Data

Data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner and is intended to be processed or is being processed or has been processed in a computer system or computer network. It may be in the form of computer printouts, magnetic or optical storage media, punched cards, punched tapes or stored internally in the memory of the computer.

Access

With its grammatical variations and similar expressions, access means gaining entry into or instructing to or communicating with the logical, arithmetical or memory resources of the computer or computer system or computer network.

Attribution

Attribution is the term which is related to the sender or the originator of the information or with the person who sends the products to the other persons or customers.

Acknowledgment

It is a term related to the receiver who receives the product from the originator or from the owner. It can be in the electronic form. The product can be acknowledged to the originator itself or to a person who has the authority to act on the behalf of the owner. The acknowledgement can be sent by an information system automatically by the owner himself or on behalf of the owner.

Public Domain Software

It is software which is not copyrighted. This means that the authors have waived copyrights over the software. Anybody can copy, modify or use the software in a manner they want. These programs can be freely incorporated into new works without paying royalties for the original material.

Freeware Software

It is free software that allows everyone to copy, redistribute and modify the software without any cost, without paying any royalty to the originator. But the copyright is hold by the original authors. Linux is an example of freeware software.

Shareware Software

It is a freely distributed and available for free testing software. One can share the software with others with owner's permission. Usually these softwares comes with a trial period (normally for about 30 days) After this trial period, if the user wants to continue with the use of software, then a registration procedure is to be carried out. The softwares which are distributed through various magazines are normally of this type.

Fair use

This is an exceptional case of copyright which allows copying of a limited amount of information freely, only in certain cases, without the permission of the copyright owner. The fair use of the information is allowed for the purpose of criticism, comment, teaching, news reporting, scholarship or research works etc. Whether a particular user is a fair user or not depends upon (a) the purpose and the character of the use (b) the nature of the copyrighted work (c) the amount and substantiality of the portion used in relation to the copyrighted work as a whole (d) the effect of the use upon the main market for the value of the copyrighted work. The main advantage of the fair use is that the public will be able to access the material without paying any fees or without asking any permission to anybody. If the partial work is implemented, then the fair use will be the best choice.

Types of unauthorized access

(a) Intentional damage to the equipment, software or data of the other users
(b) Unauthorized monitoring of electronic communication
(c) Unauthorized copying of copyrighted material
(d) Unauthorized use of computer accounts or user ids
(e) Attempt to guess or break another users passwords
(f) Change in private files in ones computer
(g) Unauthorized change in the software developed by the owner
(h) Attempt to log-in in the computer network beyond the given limits

Disadvantages of software piracy

(a) When a software is pirated, customers and software developers are harmed.
(b) With a pirated software, customers will have a risk of viruses from pirated diskettes and defective software.
(c) Customers cannot enjoy the full benefit of software package with the pirated copy.

Ethics in business

Business ethics indicates what is wrong and fight in the workplace and doing what is right in regard to effects of products or services. Ethics are to be implemented in the business in order to face the increased competition and hence to enrich one's business. For good and well going business, following guidelines are followed.

(a) Disclose an accurate information in all solicitations.
(b) Change only those fees which are in good faith estimate.
(c) Conduct the business in a manner so as to reflect honesty, honor and integrity.
(d) Do not disclose any confidential information about the business when not required.
(e) Give more attention to improve the product or the process of the organization.
(f) Try to maintain a good moral in the organization.
(g) Try to cultivate a strong teamwork and productivity in the business by designing good ethics guidelines.
(h) Try to build a good and strong image in the minds of public by designing good and healthy business ethics.

Code of ethics

Today in the computer and network systems, computer professionals and users have responsibility to provide standard of work and assure about security, privacy and control in their product or services offered to the society. With such responsibilities, it requires that all computer users and system administrators must understand the norms (rules) and principles applied to the task.

Code of ethics supplies these norms and principles. It is a way of setting standards such as commitments, responsibilities and requirements of members within the computing environment. For computer professionals and users the general code of ethics is as follows.

(a) Treat everyone fairly**.** Do not discriminate against anyone on ground such as age, post, gender etc. This is known as **Fair Treatment.**

(b) Continuously strive to honor the rights to the privacy of all the individuals. Access private information of the computer systems only when it is extremely necessary in the course of duties, that to with prior permission of the authorities. Try to maintain and protect the privacy of any confidential information. Avoid using any confidential information for your personal interest. This is known as **maintaining the privacy of the users and professionals.**

(c) Try to keep informing the users about computing matters which will affect their work conditions. Change in information such as acceptable use of resources, sharing of common resources, maintenance of security and any relevant legal obligations must be conveyed to the users from time to time. This is known as **maintaining good communication with the users.**

(d) Try to ensure the integrity of the systems. Regularly perform the maintenance of the hardware and software packages, analyze the system performance and prevent the unauthorized use or access. This is known as **maintaining good system integrity.**

(e) Try to cooperate and support your colleagues. Acknowledge the community responsibility which is most important for the integrity of the local, national and international network of computer users and computing resources. In other words try to **maintain healthy cooperation.**

(f) Be honest to yourself and to your customer. Take help of your seniors whenever necessary. Try to avoid interest conflicts if there are any. **Honesty** is one of the most important quantities in business ethics.

(g) Try to keep yourself update with the latest trends and traditions which are running in the market about your business. For this you may have to go through the training, study and information and experience sharing with your colleagues or seniors. If required help others to improve their skill and performance. Be educated and **educate** the others in your vicinity.

(h) Keep on collecting knowledge about the social and legal issues relating to computing environments. If required, communicate the changes to others and encourage them to adopt the new changes in the policies and laws about the computer systems. This quality is known as **social responsibility.**

(i) Be honest about the occurrences of the mistakes. Try to correct them in time. Never repeat the previous mistakes. Try to achieve and also maintain a safe, healthy and

productive workplace. Try to maintain the quality of your product and the services related to it, always to the optimum level.

(j) Try to maintain a consistency in maintaining the good ethical standards and the best degree of professionalism in yourself while performing your duties. This is known as **ethical responsibility.**

(k) Allow individuals to inspect and correct personal information. Try to remove any wrong data associated with any individual. Be prompt in taking such decisions.

Do's and Don'ts for the ethics culture of the computer professionals

Do's:

(a) Internet is a huge source of authentic and accurate information. Make use of this facility to explore and enhance your knowledge.

(b) Do use internet to communicate good and important messages.

(c) Do use the internet to visit the web sites which will enrich your knowledge.

(d) In a computer network, talk with 'strangers' with atmost care.

(e) Do respect the privacy of the others while you are on the net.

(f) 'Download' the programs or softwares from the net with atmost care.

(g) Always make use of a licensed antivirus program, properly installed on your computer.

(h) Use internet to learn more and more about the world and the incidences which are happenings in the world around you.

Don'ts:

(a) Don't give your internet account password, computers / systems password to anyone. Passwords are meant for protection of your computer and the data in your computer.

(b) Don't answer any messages which you feel to be improper, threatening or about which you feel uncomfortable.

(c) Don't arrange to meet any unauthorized person with whom you had a meeting on net.

(d) Don't give any personal information such as your family's address, phone numbers, credit card numbers and calling card numbers to any unknown person on a computer network.

(e) Don't try to break into computers. It's a crime. It's an invasion of privacy. Computers often contain certain sensitive information. Don't try to access it, if it is not related with u.

(f) Don't try to use any authentic software without the permission of the owner. i.e. In other words, don't use any pirated software. Don't download it from the net.

(g) Don't make duplication of any copyrighted material such as books or magazines without the permission of the author or publisher.

Ethics Guidelines

These are based on the information technique, privacy, good and healthy use and good and healthy sharing of resources, common sense and politeness to protect privacy and to ensure that everyone has same access to the resources. These are as follows:

(a) **Misuse of computer resources:** Misuse of any computer hardware or software will be regarded as illegal of unethical behavior.

(b) **Use of good and healthy communication facilities:** Users should use the various facilities provided on the net such as e-mail, bulletin boards, newsgroups etc for the very basic purpose for which these are designed for. Use of these facilities for commercial or political purposes is strictly prohibited. Random mailing of threatening and harassing messages should be strictly avoided.

(c) **Respect laws and copyrights:** Always follow the copyright protections given to the softwares and their users. It is against the policy to copy or reproduce any licensed equipment except it is explicitly permitted by the software license.

(d) **Unauthorized access of data:** Without permission of the authorities, users should not brows or access or even change the private files on the computers nor they should try to modify the computer systems or the softwares there in.

(e) **Do not share your account or password:** The user should not share his/her account or password with someone else, howsoever close he/her might be.

(f) **Respect the privacy of the other users:** Users should not intentionally look into the personal information of other person or even try to modify the same. If by some reasons you have to give password to the other users, then once that job is over, change the password immediately.

(g) **Fair use of computer hardware and software facility:** Users have to maintain their accounts, user-ids, passwords on their own. These should be used only for the stated authentic purpose and not for the other.

Ethics for computer professionals

(a) All computer users have the responsibility to use computer system with an effective, efficient, ethical and lawful manner. They are expected to maintain professional standards. Follow the professional responsibility and also the programmer's liability.

(b) Computer professionals are expected to maintain the expected standard in their software. The professionals must test and prove these standards physically.

(c) Computer professionals must strive continuously to honor the rights of the privacy of all individuals. They should provide the means to protect their data from unauthorized access.

(d) Computer professionals should disclose the contents only to the concerned authorities. They must maintain data confidentiality.

(e) Computer professionals should not use the personal information content obtained for one specific purpose to another purpose without prior permission of the concerned authorities.

(f) Computer professionals should take atmost care of accuracy, reliability and completeness of the data. i.e. in other words, they should promote the data integrity.

(g) Computer professionals should follow the standard methods of record keeping practices and data use. i.e. in other words they should allow data inspection from time to time regularly.

(h) The computer professional must bind himself/herself to achieve the best quality in the product.

(i) The computer programmer / professional must know and respect the existing laws and regulations and must obey them while developing the software on local, national or international level.

Programmer's Liability

(a) A programmer should be aware of the bugs in the program.
(b) A programmer should have a fair intension for developing a program to give best solution for the problem.
(c) If required, the programmer should take the help from the appropriate experts from appropriate fields so as to deliver the best for the consumer.

Intellectual Property Rights

These deals with the issues in the copyright and patent laws that provides incentive to the inventor. To protect inventors and to prosecute individuals who undertake illegal acts, new laws are formed. If inventors cannot get a return on their investment in developing new products, they will lose their interest in developing the new product and will result in the loss of the society. If the customers want to obtain a copy of the product or the software, then they have to pay for it. Intellectual property rights are related to copyright, fair use of the product, copying and distributing limitations and attribution and acknowledgement.

Copyrights

Copyright is an intellectual property right attached to original works in which the right-subsist with him. Copyright is a form of protection provided by the law to the authors of 'original works of authorship' including literacy, dramatic, musical, artistic and certain other intellectual works. This protection is available in both published and unpublished works. Copyright law is useful for authorship determination, duration of protection and requirements for transfers of rights to others. Copyright is the exclusive right to do or to authorize the others to do the following acts in respect of the original work.

To perform work in public

(a) To make any movie film or sound recording in respect of the work
(b) To make any translation of the work
(c) To reproduce the work in any material form or storing of it in any medium by electronic means
(d) To make any adaptation of the work

It is illegal for anyone to violate any of the rights provided by the act to the owner of copyright. Copyright protection begins when any of the work is actually created and fixed in a suitable form. If one develops any work originally, then one can place the copyright symbol © next to your name. For example: Copyright© 2006 HYS

Ten commandments of computing

Ethical principles are codified into a set of "commandments for computer users and professionals". Ten Commandments of computing are as follows:

(a) One should not use a computer to harm other people.
(b) One should not interfere with neighbor's computer work.
(c) One should not watch around the neighbor's computer files.
(d) One should not use a computer for the purpose of steal.
(e) One should not use a computer to bear a false witness.
(f) One should not copy or use the software for which one has not paid.
(g) One should not use other person's computer resources without authentication or without proper authorization.
(h) One should not appropriate other person's intellectual output.
(i) One should think about the social awareness and consequence of the program the one is writing or the system the one is designing.

(j) One should always use a computer by means that show due considerations and due respect for one's fellow humans.

Important contents of IT act of India. Or Information Technology Act 2000.

Information Technology Act 2000 is an act to provide legal recognition for internet and e-commerce. It contains the following chapters.

(1) Preliminary:

With the rapid pace, internet usage in India is increasing. So the rule of government is to provide a legal framework for internet and e-commerce.

(2) Electronic Governance:

The filling up of a form, issue of a license or payment of fee may be in an electronic form. Secured digital signatures enables the growth of e-commerce.

(3) Attribution, Acknowledgement and Dispatch of Electronic Records:

This chapter of the Act specifies the time of dispatch and receipt ot electronic record. An electronic record with a secure digital signature will automatically be considered as a secure electronic record. It will also be considered as a secure if security procedures have been applied to it. Such security may be in the form of encryption.

(4) Regulation of certifying Authorities:

"Certifying Authority" means a person who has been granted a license to issue a Digital Signature Certificate under section24.

(5) Digital Signature Certificate:

It means a certificate issued under sub-section (4) of section 35

(6) Duties of Subscribers:

Subscriber checks any electronic record by means of an electronic method or procedure.

(7) Penalties and Adjudication:

The penalty for tampering source code is imprisonment for a term not exceeding 3 years and/or a fine not exceeding Rs. 200000. In order to enforce the punishments, central government will appoint an Adjucating Officer who will have powers of civil court.

(8) The Cyber Regulations Appellate Tribunal:

The Act contemplates the constitution of the Cyber regulation Appellate Tribunal, having a Presiding Officer. Tribunal will hear appeals from orders passed by Adjucating Officer. The party may appeal to High Court of any state within 60 days, if unsatisfied with the order of Tribunal.

(9) Definitions.:

In these Rules, unless the context otherwise requires

(a) "**Act**" means the Information Technology Act, 2000 (21 of 2000);

(b) "**applicant**" means Certifying Authority applicant;

(c) "**auditor**" means any internationally accredited computer security professional or agency appointed by the Certifying Authority and recognized by the Controller for conducting technical audit of operation of Certifying Authority;

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

(e) "**Information asset**" means all information resources utilized in the course of any organization's business and includes all information, applications (software developed or purchased), and technology (hardware, system software and networks);
(f) "**Licensee**" means a licence granted to Certifying Authorities for the issue of Digital Signature Certificates under these rules;
(g) "**Licensed Certifying Authority**" means Certifying Authority who has been granted a licence to issue Digital Signature Certificates;
(h) "**Person**" shall include an individual; or a company or association or body of individuals; whether incorporated or not; or Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments;
(i) "**Schedule**" means a schedule annexed to these rules;
(j) "**Subscriber identity verification method**" means the method used to verify and authenticate the identity of a subscriber;
(k) "**Trusted person**" means any person who has: (i) direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or these Rules in respect of a Certifying Authority; or (ii) duties directly involving the issuance, renewal, suspension, revocation of Digital Signature Certificates (including the identification of any person requesting a Digital Signature Certificate from a licensed Certifying Authority), creation of private keys or administration of a Certifying Authority's computing facilities.
(10) The manner in which information be authenticated by means of Digital Signature.- A **Digital Signature** shall,-
(a) be created and verified by cryptography that concerns itself with transforming electronic record into seemingly unintelligible forms and back again;
(b) use what is known as "Public Key Cryptography", which employs an algorithm using two different but mathematical related "keys" – one for creating a Digital Signature or transforming data into a seemingly unintelligible form, and another key for verifying a Digital Signature or returning the electronic record to original form, the process termed as hash function shall be used in both creating and verifying a Digital Signature. Explanation: Computer equipment and software utilizing two such keys are often termed as "asymmetric cryptography".
(11) Creation of Digital Signature.-
To sign an electronic record or any other item of information, the signer shall first apply the hash function in the signer's software; the hash function shall compute a hash result of standard length which is unique (for all practical purposes) to the electronic record; the signer's software transforming the hash result into a Digital Signature using signer's private key; the resulting Digital Signature shall be unique to both electronic record and private key used to create it; and the Digital Signature shall be attached to its electronic record and stored or transmitted with its electronic record.
(12) Verification of Digital Signature :
The verification of a Digital Signature shall be accomplished by computing a new hash result of the original electronic record by means of the hash function used to create a Digital Signature and by using the public key and the new hash result, the verifier shall check- (i) if the Digital Signature was created using the corresponding private key; and (ii) if the newly computed hash result matches the original result which was transformed into

Digital Signature during the signing process. The verification software will confirm the Digital Signature as verified if:- (a)the signer's private key was used to digitally sign the electronic record, which is known to be the case if the signer's public key was used to verify the signature because the signer's public key will verify only a Digital Signature created with the signer's private key; and (b) the electronic record was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the Digital Signature during the verification process.

(13) Expiry of Digital Signature Certificate :

(1) A Digital Signature Certificate (a) shall be issued with a designated expiry date; (b) which is suspended shall return to the operational use, if the suspension is withdrawn in accordance with the provisions of section 37 of the Act; (c) shall expire automatically upon reaching the designated expiry date at which time the Digital Signature Certificate shall be archived; (d) on expiry, shall not be re-used. (2) The period for which a Digital Signature Certificate has been issued shall not be extended, but a new Digital Signature Certificate may be issued after the expiry of such period.

(14) Information Management : System Administration :

(1) Each organization shall designate a properly trained "System Administrator" who will ensure that the protective security measures of the system are functional and who will maintain its security posture. Depending upon the complexity and security needs of a system or application, the System Administrator may have a designated System Security Administrator who will assume security responsibilities and provide physical, logical and procedural safeguards for information.

(2) Organizations shall ensure that only a properly trained System Security Administrator is assigned the system security responsibilities.

(3) The responsibility to create, classify, retrieve, modify, delete or archive information must rest only with the System Administrator.

(4) Any password used for the system administration and operation of trusted services must not be written down (in paper or electronic form) or shared with any one. A system for password management should be put in place to cover the eventualities such as forgotten password or changeover to another person in case of System Administrator (or System Security Administrator) leaving the organization. Every instance of usage of administrator's passwords must be documented.

(5) Periodic review of the access rights of all users must be performed.

(6) The System Administrator must promptly disable access to a user's account if the user is identified as having left the Data Centre, changed assignments, or is no longer requiring system access. Reactivation of the user's account must be authorized in writing by the System Administrator (Digitally signed e-mail may be acceptable).

(7) The System Administrator must take steps to safeguards classified information as prescribed by its owner.

(8) The System Administrator must authorize privileged access to users only on a need-to-know and need-to-do basis and also only after the authorization is documented.

(9) Criteria for the review of audit trails/access logs, reporting of access violations and procedures to ensure timely management action/response shall be established and documented.

(10) All security violations must be recorded, investigated, and periodic status reports

compiled for review by the management.
(11) The System Administrator together with the system support staff shall conduct a regular analysis of problems reported to and identify any weaknesses in protection of the information.
(12) The System Administrator shall ensure that the data, file and Public Key Infrastructure (PKI) servers are not left unmonitored while these systems are powered on.
(13) The System Administrator should ensure that no generic user is enabled or active on the system.

(15) Sensitive Information Control

(1) Information assets shall be classified and protected according to their sensitivity and criticality to the organization.
(2) Procedures in accordance with para 8.3 of these Guidelines must be in place to handle the storage media, which has sensitive and classified information.
(3) All sensitive information stored in any media shall bear or be assigned an appropriate security classification.
(4) All sensitive material shall be stamped or labeled accordingly.
(5) Storage media (i.e. floppy diskettes, magnetic tapes, portable hard disks, optical disks, etc. containing sensitive information shall be secured according to their classification.
(6) Electronic communication systems, such as router, switches, network device and computers, used for transmission of sensitive information should be equipped or installed with suitable security software and if necessary with an encryptor or encryption software. The appropriate procedure in this regard should be documented.
(7) Procedures shall be in place to ensure the secure disposal of sensitive information assets on all corrupted/damaged or affected media both internal (e.g. hard disk/optical disk) and external (e.g. diskette, disk drive, tapes etc.) to the system. Preferably such affected/corrupted/damaged media both internal and external to the system shall be destroyed.

(16) Sensitive Information Security

(1) Highly sensitive information assets shall be stored on secure removable media and should be in an encrypted format to avoid compromise by unauthorized persons.
(2) Highly sensitive information shall be classified in accordance with para 3.
(3) Sensitive information and data, which are stored on the fixed disk of a computer shared by more than one person, must be protected by access control software (e.g., password). Security packages must be installed which partition or provide authorization to segregated directories/files.
(4) Removable electronic storage media must be removed from the computer and properly secured at the end of the work session or workday.
(5) Removable electronic storage media containing sensitive information and data must be clearly labeled and secured.
(6) Hard disks containing sensitive information and data must be securely erased prior to giving the computer system to another internal or external department or for maintenance.

(17) Third Party Access

(1) Access to the computer systems by other organizations shall be subjected to a similar level of security protection and controls as in these Information Technology security

guidelines.
(2) In case the Data Centre uses the facilities of external service/facility provider (outsourcer) for any of their operations, the use of external service/facility providers (e.g. outsourcer) shall be evaluated in light of the possible security exposures and risks involved and all such agreements shall be approved by the information asset owner. The external service or facility provider shall also sign non-disclosure agreements with the management of the Data Centre/operational site.
(3) The external service/facility provider (e.g. outsourcer) shall provide an equivalent level of security controls as required by these Information Technology Security Guidelines.

(18) Prevention of Computer Misuse

(1) Prevention, detection, and deterrence measures shall be implemented to safeguard the security of computers and computer information from misuse. The measures taken shall be properly documented and reviewed regularly.
(2) Each organization shall provide adequate information to all persons, including management, systems developers and programmers, end users, and third party users warning them against misuse of computers.
(3) Effective measures to deal expeditiously with breaches of security shall be established within each organization. Such measures shall include :
(i) Prompt reporting of suspected breach; (ii) Proper investigation and assessment of the nature of suspected breach; (iii) Secure evidence and preserve integrity of such material as relates to the discovery of any breach; (iv) Remedial measures.
(4) All incidents related to breaches shall be reported to the System Administrator or System Security Administrator for appropriate action to prevent future occurrence.
(5) Procedure shall be set-up to establish the nature of any alleged abuse and determine the subsequent action required to be taken to prevent its future occurrence. Such procedures shall include: (i) The role of the System Administrator, System Security Administrator and management; (ii) Procedure for investigation; (iii) Areas for security review; and (iv) Subsequent follow-up action.

(19) Use of Security Systems or Facilities

(1) Security controls shall be installed and maintained on each computer system or computer node to prevent unauthorized users from gaining entry to the information system and to prevent unauthorized access to data.
(2) Any system software or resource of the computer system should only be accessible after being authenticated by access control system.

(20) System Access Control

(1) Access control software and system software security features shall be implemented to protect resources. Management approval is required to authorize issuance of user identification (ID) and resource privileges.
(2) Access to information system resources like memory, storage devices etc. Sensitive utilities and data resources and program files shall be controlled and restricted based on a "need-to-use" basis with proper segregation of duties.
(3) The access control software or operating system of the computer system shall provide features to restrict access to the system and data resources. The use of common passwords such as “administrator” or “president” or “game” etc. to protect access to the system and data resources represent a security exposure and shall be avoided. All passwords used

must be resistant to dictionary attacks.
(4) Appropriate approval for the request to access system resources shall be obtained from the System Administrator. Guidelines and procedures governing access authorizations shall be developed, documented and implemented.
(5) An Access Control System manual documenting the access granted to different level of users shall be prepared to provide guidance to the System Administrator for grant of access.
(6) Each user shall be assigned a unique user ID. Adequate user education shall be provided to help users in password choice and password protection. Sharing of user IDs shall not be allowed.
(7) Stored passwords shall be encrypted using internationally proven encryption techniques to prevent unauthorized disclosure and modification.
(8) Stored passwords shall be protected by access controls from unauthorized disclosure and modification.
(9) Automatic time-out for terminal inactivity should be implemented.
(10) Audit trail of security-sensitive access and actions taken shall be logged.
(11) All forms of audit trail shall be appropriately protected against unauthorized modification or deletion.
(12) Where a second level access control is implemented through the application system, password controls similar to those implemented for the computer system shall be in place.
(13) Activities of all remote users shall be logged and monitored closely.
(14) The facility to login as another user from one user's login shall be denied. However, the system should prohibit direct login as a trusted user (e.g. root in
Unix, administrator in Windows NT or Windows 2000). This means that there must be a user account configured for the trusted administrator. The system requires trusted users to change their effective username to gain access to root and to re-authenticate themselves before requesting access to privileged functions.
(15) The startup and shutdown procedure of the security software must be automated.
(16) Sensitive Operating System files which are more prone to hackers must be protected against all known attacks using proven tools and techniques. That is
to say no user will be able to modify them except with the permission of System Administrator.

(21) Password Management

(1) Certain minimum quality standards for password shall be enforced. The quality level shall be increased progressively. The following control features shall be implemented for passwords:
(i) Minimum of eight characters without leading or trailing blanks; (ii) Shall be different from the existing password and the two previous ones; (iii) Shall be changed at least once every ninety days; for sensitive system, password shall be changed at least once every thirty days; and (iv) Shall not be shared, displayed or printed.
(2) Password retries shall be limited to a maximum of three attempted logons after which the user ID shall then be revoked; for sensitive systems, the number of password retries should be limited to a maximum of two.
(3) Passwords which are easy-to-guess (e.g. user name, birth date, month, standard words etc.) should be avoided.

(4) Initial or reset passwords must be changed by the user upon first use.
(5) Passwords shall always be encrypted in storage to prevent unauthorized disclosure.
(6) All passwords used must be resistant to dictionary attacks and all known password cracking algorithms.

(22) Privileged User's Management

(1) System privileges shall be granted to users only on a need-to-use basis.
(2) Login privileges for highly privileged accounts should be available only from Console and terminals situated within Console room.
(3) An audit trail of activities conducted by highly privileged users shall be maintained for two years and reviewed periodically at least every week by operator who is independent of System Administrator.
(4) Privileged user shall not be allowed to log in to the computer system from remote terminal. The usage of the computer system by the privilege user shall be allowed during a certain time period.
(5) Separate user IDs shall be allowed to the user for performing privileged and normal (non-privileged) activities.
(6) The use of user IDs for emergency use shall be recorded and approved. The passwords shall be reset after use.

(23) User's Account Management

(1) Procedures for user account management shall be established to control access to application systems and data. The procedures shall include the following:
(i) Users shall be authorized by the computer system owner to access the computer services. (ii) A written statement of access rights shall be given to all users.
(iii) All users shall be required to sign an undertaking to acknowledge that they understand the conditions of access. (iv) Where access to computer services is administered by service providers, ensure that the service providers do not provide access until the authorization procedures have been completed. This includes the acknowledgement of receipt of the accounts by the users. (v) A formal record of all registered users of the computer services shall be maintained. (vi) Access rights of users who have been transferred, or left the organization shall be removed immediately. (vii) A periodic check shall be carried out for redundant user accounts and access rights that are no longer required. (viii) Ensure that redundant user accounts are not re-issued to another user.
(2) User accounts shall be suspended under the following conditions:
(i) When an individual is on extended leave or inactive use of over thirty days. In case of protected computer system, the limit of thirty days may be reduced to fifteen days by the System Administrator. (ii) Immediately upon the termination of the services of an individual. (iii) Suspended or inactive accounts shall be deleted after a two months period. In case of protected computer systems, the limit of two months may be reduced to one month.

(24) Data and Resource Protection

(1) All information assets shall be assigned an "owner" responsible for the integrity of that data/resource. Custodians shall be assigned and shall be jointly responsible for information assets by providing computer controls to assist owners.
(2) The operating system or security system of the computer system shall: (i) Define user authority and enforce access control to data within the computer system; (ii) Be capable of

specifying, for each named individual, a list of named data objects (e.g. file, program) or groups of named objects, and the type of access allowed.
(3) For networked or shared computer systems, system users shall be limited to a profile of data objects required to perform their needed tasks.
(4) Access controls for any data and/or resources shall be determined as part of the systems analysis and design process.
(5) Application Programmer shall not be allowed to access the production system.

(25) Sensitive Systems Protection

(1) Security tokens/smart cards/bio-metric technologies such as Iris recognition, finger print verification technologies etc. shall be used to complement the usage of passwords to access the computer system.
(2) For computer system processing sensitive data, access by other organizations shall be prohibited or strictly controlled.
(3) For sensitive data, encryption of data in storage shall be considered to protect its confidentiality and integrity.

(26) Job Scheduling

(1) Procedures shall be established to ensure that all changes to the job schedules are appropriately approved. The authority to approve changes to job schedules shall be clearly assigned.
(2) As far as possible, automated job scheduling should be used. Manual job scheduling should require prior approval from the competent authority.

(27) System Operations Procedure

(1) Procedures shall be established to ensure that only authorized and correct job stream and parameter changes are made.
(2) Procedures shall be established to maintain logs of system activities. Such logs shall be reviewed by a competent independent party for indications of dubious activities. Appropriate retention periods shall be set for such logs.
(3) Procedures shall be established to ensure that people other than well trained computer operators are prohibited from operating the computer equipment.
(4) Procedures shall be implemented to ensure the secure storage or distribution of all outputs/reports, in accordance with procedures defined by the owners for each system.

(28) Media Management

(1) Responsibilities for media library management and protection shall be clearly defined and assigned.
(2) All media containing sensitive data shall be stored in a locked room or cabinets, which must be fire resistant and free of toxic chemicals.
(3) Access to the media library (both on-site and off-site) shall be restricted to the authorized persons only. A list of personnel authorized to enter the library shall be maintained.
(4) The media containing sensitive and back up data must be stored at three different physical locations in the country, which can be reached in few hours.
(5) A media management system shall be in place to account for all media stored on-site and off-site.
(6) All incoming/outgoing media transfers shall be authorized by management and users.

(7) An independent physical inventory check of all media shall be conducted at least every six months.
(8) All media shall have external volume identification. Internal labels shall be fixed, where available.
(9) Procedures shall be in place to ensure that only authorized addition/removal of media from the library is allowed.
(10) Media retention periods shall be established and approved by management in accordance with legal/regulatory and user requirements.

(29) Media Movement

(1) Proper records of all movements of computer tapes/disks between onsite and off-site media library must be maintained.
(2) There shall be procedures to ensure the authorized and secure transfer to media to/from external parties and the off-site location. A means to authenticate the receipt shall be in place.
(3) Computer media that are being transported to off-site data backup locations should be stored in locked carrying cases that provide magnetic field protection and protection from impact while loading and unloading and during transportation.

(30) Data Backup and Off-site Retention

(1) Back-up procedures shall be documented, scheduled and monitored.
(2) Up-to-date backups of all critical items shall be maintained to ensure the continued provision of the minimum essential level of service. These items include:
(i) Data files (ii) Utilities programs (iii) Databases (iv) Operating system software (v) Applications system software (vi) Encryption keys (vii) Pre-printed forms
(viii) Documentation (including a copy of the business continuity plans)
(3) One set of the original disks for all operating system and application software must be maintained to ensure that a valid, virus-free backup exists and is available for use at any time.
(4) Backups of the system, application and data shall be performed on a regular basis. Backups should also be made for application under development and data conversion efforts.
(5) Data backup is required for all systems including personal computers, servers and distributed systems and databases.
(6) Critical system data and file server software must have full backups taken weekly.
(7) The backups must be kept in an area physically separate from the server. If critical system data on the LAN represents unique versions of the information assets, then the information backups must be rotated on a periodic basis to an off-site storage location.
(8) Critical system data and file server software must have incremental backups taken daily.
(9) Systems that are completely static may not require periodic backup, but shall be backed up after changes or updates in the information.
(10) Each LAN/system should have a primary and backup operator to ensure continuity of business operations.
(11) The business recovery plan should be prepared and tested on an annual basis.

(31) Measures to Handle Computer Virus

(1) Responsibilities and duties shall be assigned to ensure that all file servers and personal

computers are equipped with up-to-date virus protection and detection software.
(2) Virus detection software must be used to check storage drives both internal and external to the system on a periodic basis.
(3) All diskettes and software shall be screened and verified by virus detection software before being loaded onto the computer system. No magnetic media like tape cartridge, floppies etc. brought from outside shall be used on the data, file, or computer server or personal computer on Intranet and Internet without proper screening and verification by virus detection software.
(4) A team shall be designated to deal with reported or suspected incidents of computer virus. The designated team shall ensure that latest version of anti-virus software is loaded on all data, file, PKI servers and personal computers.
(5) Procedures shall be established to limit the spread of viruses to other organization information assets. Such procedures inter alias shall include: (i) Communication to other business partners and users who may be at risk from an infected resource (ii) Eradication and recovery procedures (iii) Incident report must be documented and communicated per established procedures.
(6) An awareness and training programme shall be established to communicate virus protection practices, available controls, areas of high risk to virus infection and responsibilities.

(32) Relocation of Hardware and Software

Whenever computers or computer peripherals are relocated (e.g. for maintenance, installation at different sites or storage), the following guidelines shall apply:
(i) All removable media will be removed from the computer system and kept at secure location. (ii) Internal drives will be overwritten, reformatted or removed as the situation may be. (iii) If applicable, ribbons will be removed from printers. (iv) All paper will be removed from printers.

(33) Hardware and Software Maintenance

Whenever, the hardware and software maintenance of the computer or computer network is being carried out, the following should be considered:
(1) Proper placement and installation of Information Technology equipment to reduce the effects of interference due to electromagnetic emanations.
(2) Maintenance of an inventory and configuration chart of hardware.
(3) Identification and use of security features implemented within hardware.
(4) Authorization, documentation, and control of change made to the hardware.
(5) Identification of support facilities including power and air conditioning.
(6) Provision of an uninterruptible power supply.
(7) Maintenance of equipment and services.
(8) Organization must make proper arrangements for maintenance of computer hardware, software (both system and application) and firmware installed and used by them. It shall be the responsibility of the officer in charge of the operational site to ensure that contract for annual maintenance of hardware is always in place.
(9) Organization must enter into maintenance agreements, if necessary, with the supplier of computer and communication hardware, software (both system and application) and firmware.
(10) Maintenance personnel will sign non-disclosure agreements.

(11) The identities of all hardware and software vendor maintenance staff should be verified before allowing them to carry out maintenance work.
(12) All maintenance personnel should be escorted within the operational site/computer system and network installation room by the authorized personnel of the organization.
(13) After maintenance, any exposed security parameters such as passwords, user IDs, and accounts will be changed or reset to eliminate any potential security exposures.
(14) If the computer system, computer network or any of its devices is vulnerable to computer viruses as a result of performing maintenance, system managers or users shall scan the computer system and its devices and any media affected for viruses as a result of maintenance.

(34) Purchase and Licensing of Hardware and Software

(1) Hardware and software products that contain or are to be used to enforce security, and intended for use or interface into any organization system or network, must be verified to comply with these Information Technology Security Guidelines prior to the signing of any contract, purchase or lease.
(2) Software, which is capable of bypassing or modifying the security system or operating system, integrity features, must be verified to determine that they conform to these Information Technology Security Guidelines. Where such compliance is not possible, then procedures shall be in place to ensure that the implementation and operation of that software does not compromise the security of the system.
(3) There shall be procedures to identify, select, implement and control software (system and application software) acquisition and installation to ensure compliance with the Indian Copyright Act and Information Technology Security Guidelines.
(4) It is prohibited to knowingly install on any system whether test or production, any software which is not licensed for use on the specific systems or networks.
(5) No software will be installed and used on the system when appropriate licensing agreements do not exist, except during evaluation periods for which the user has documented permission to install and test the software under evaluation.
(6) Illegally acquired or unauthorized software must not be used on any computer, computer network or data communication equipment. In the event that any illegally acquired or unauthorized software is detected by the System Administrator or Network Administrator, the same must be removed immediately.

(35) System Software

(1) All system software options and parameters shall be reviewed and approved by the management.
(2) System software shall be comprehensively tested and its security functionality validated prior to implementation.
(3) All vendor supplied default user IDs shall be deleted or password changed before allowing users to access the computer system.
(4) Versions of system software installed on the computer system and communication devices shall be regularly updated.
(5) All changes proposed in the system software must be appropriately justified and approved by an authorized party.
(6) A log of all changes to system software shall be maintained, completely documented and tested to ensure the desired results.

(7) Procedures to control changes initiated by vendors shall be in accordance with para 21 pertaining to "Change Management ".
(8) There shall be no standing "Write" access to the system libraries. All "Write" access shall be logged and reviewed by the System Administrator for dubious activities.
(9) System Programmers shall not be allowed to have access to the application system's data and programme files in the production environment.
(10) Procedures to control the use of sensitive system utilities and system programs that could bypass intended security controls shall be in place and documented. All usage shall be logged and reviewed by the System Administrator and another person independent of System Administrator for dubious activities.

(36) Documentation Security

(1) All documentation pertaining to application software and sensitive system software and changes made therein shall be updated to the current time, accurately and stored securely. An up-to-date inventory list of all documentation shall be maintained to ensure control and accountability.
(2) All documentation and subsequent changes shall be reviewed and approved by an independent authorized party prior to issue.
(3) Access to application software documentation and sensitive system software documentation shall be restricted to authorized personnel on a "need-to-use" basis only.
(4) Adequate backups of all documentation shall be maintained and a copy of all critical documentation and manuals shall be stored off-site.
(5) Documentation shall be classified according to the sensitivity of its contents/implications.
(6) Organizations shall adopt a clean desk policy for papers, diskettes and other documentation in order to reduce the risks of unauthorized access, loss of and damage to information outside normal working hours.

(37) Network Communication Security

(1) All sensitive information on the network shall be protected by using appropriate techniques. The critical network devices such as routers, switches and modems should be protected from physical damage.
(2) The network configuration and inventories shall be documented and maintained.
(3) Prior authorization of the Network Administrator shall be obtained for making any changes to the network configuration. The changes made in the network configuration shall be documented. The threat and risk assessment of the network after changes in the network configuration shall be reviewed. The network operation shall be monitored for any security irregularity. A formal procedure should be in place for identifying and resolving security problems.
(4) Physical access to communications and network sites shall be controlled and restricted to authorized individuals only in accordance with para 4.4 pertaining to “Physical Access”.
(5) Communication and network systems shall be controlled and restricted to authorized individuals only in accordance with para 6.2 – System Access Control.
(6) As far as possible, transmission medium within the Certifying Authority’s operational site should be secured against electromagnetic transmission. In this regard, use of Optical Fibre Cable and armored cable may be preferred as transmission media as the case may

be.
(7) Network diagnostic tools, e.g., spectrum analyzer, protocol analyzer should be used on a need basis.

(38) Firewalls

(1) Intelligent devices generally known as "Firewalls" shall be used to isolate organization's data network with the external network. Firewall device should also be used to limit network connectivity for unauthorized use.
(2) Networks that operate at varying security levels shall be isolated from each other by appropriate firewalls. The internal network of the organization shall be physically and logically isolated from the Internet and any other external connection by a firewall.
(3) All firewalls shall be subjected to thorough test for vulnerability prior to being put to use and at least half-yearly thereafter.
(4) All web servers for access by Internet users shall be isolated from other data and host servers.

(39) Connectivity

(1) Organization shall establish procedure for allowing connectivity of their computer network or computer system to non organization computer system or networks. The permission to connect other networks and computer system shall be approved by the Network Administrator and documented.
(2) All unused connections and network segments should be disconnected from active networks. The computer system/personal computer or outside terminal accessing an organization's host system must adhere to the general system security and access control guidelines.
(3) The suitability of new hardware/software particularly the protocol compatibility should be assessed before connecting the same to the organization's network.
(4) As far as possible, no Internet access should be allowed to database server/ file server or server hosting sensitive data.
(5) The level of protection for communication and network resources should be commensurate with the criticality and sensitivity of the data transmitted.

(40) Network Administrator

(1) Each organization shall designate a properly trained "Network Administrator" who will be responsible for operation, monitoring security and functioning of the network.
(2) Network Administrator shall regularly undertake the review of network and also take adequate measures to provide physical, logical and procedural safeguards for its security. Appropriate follow up of any unusual activity or pattern of access on the computer network shall be investigated promptly by the Network Administrator.
(3) System must include a mechanism for alerting the Network Administrator of possible breaches in security, e.g., unauthorized access, virus infection and hacking.
(4) Secure Network Management System should be implemented to monitor functioning of the computer network. Broadcast of network traffic should be minimized.
(5) Only authorized and legal software shall be used on the network.
(6) Shared computer systems, network devices used for business applications shall comply with the requirement established in para 6 – System Integrity and Security Measures.

(41) Private Key Protection and Backup

(1) The Certifying Authority must protect its private keys from disclosure.

(2) The Certifying Authority must back-up its private keys. Backed-up keys must be stored in encrypted form and protected at a level no lower than those followed for storing the primary version of the key.
(3) The Certifying Authority's private key backups should be stored in a secure storage facility, away from where the original key is stored.

(42) Method of Destroying Private Key

Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be securely destroyed by over-writing. Private key destruction procedures must be described in the Certification Practice Statement or other publicly available document.

(43) Key Change

(1) Certifying Authority and Subscriber keys shall be changed periodically.
(2) Key change shall be processed as per Key Generation guidelines.
(3) The Certifying Authority shall provide reasonable notice to the Subscriber's relying parties of any change to a new key pair used by the Certifying Authority to sign Digital Signature Certificates.
(4) The Certifying Authority shall define its key change process that ensures reliability of the process by showing how the generation of key interlocks – such as signing a hash of the new key with the old key. All keys must have validity periods of no more than five years. Suggested validity period:
(a) Certifying Authority's root keys and associated certificates – five years; (b) Certifying Authority's private signing key - two years; (c) Subscriber Digital Signature Certificate key – three years; (d) Subscriber private key – three years. Use of particular key lengths should be determined in accordance with departmental Threat-Risk Assessments.

(44) Destruction

Upon termination of use of a Certifying Authority signature private key, all components of the private key and all its backup copies shall be securely destroyed.

(45) Key Compromise

(1) A procedure shall be pre-established to handle cases where a compromise of the Certifying Authority's Digital Signature private key has occurred. In such case, the Certifying Authority shall immediately revoke all affected Subscriber Digital Signature Certificates.
(2) The Certifying Authority should immediately revoke the affected keys and Digital Signature Certificates in the case of Subscriber private key compromise.
(3) The Certifying Authority's public keys shall be archived permanently to facilitate audit or investigation requirements.
(4) Archives of Certifying Authority's public keys shall be protected from unauthorized modification.

(46) Confidentiality of Subscriber's Information

(1) Procedures and security controls to protect the privacy and confidentiality of the subscribers' data under the Certifying Authority's custody shall be implemented. Confidential information provided by the subscriber must not be disclosed to a third party without the subscribers' consent, unless the information is required to be disclosed under the law or a court order.
(2) Data on the usage of the Digital Signature Certificates by the subscribers and other

transactional data relating to the subscribers' activities generated by the Certifying Authority in the course of its operation shall be protected to ensure the subscribers' privacy.

(3) A secure communication channel between the Certifying Authority and its subscribers shall be established to ensure the authenticity, integrity and confidentiality of the exchanges (e.g. transmission of Digital Signature Certificate, password, private key) during the Digital Signature Certificate issuance process.

****