CERTIFYING AUTHORITIES RULES, 2000

Government of India
Ministry of Information Technology
New Delhi, the 17th October, 2000
NOTIFICATION

G.S.R 789(E) In exercise of the powers conferred by section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules regulating the application and other guidelines for Certifying Authorities, namely:-

1. Short title and commencement
(1) These Rules may be called Information Technology (Certifying Authorities) Rules, 2000.
(2)They shall come into force on the date of their publication in the Official Gazette.

2. Definitions.- In these Rules, unless the context otherwise require
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."**Digital Signature Certificate**" means Digital Signature Certificate issued under sub-section (4) of section 35 of the Act;
f."**Information asset**" means all information resources utilized in the course of any organisation?s business and includes all information, applications (software developed or purchased), and technology (hardware, system software and networks);
g."**Licence**" means a licence granted to Certifying Authorities for the issue of Digital Signature Certificates under these rules;
h."**Licensed Certifying Authority**" means Certifying Authority who has been granted a licence to issue Digital Signature Certificates;
i."**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;
j."**Schedule**" means a schedule annexed to these rules;
k."**Subscriber identity verification method**" means the method used to verify and authenticate the identity of a subscriber;
l.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.
(m) words and expressions used herein and not defined but defined in Schedule-IV shall have the meaning respectively assigned to them in that schedule.

3. 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".

4. 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.

5. 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.

6. Standards.-The Information Technology (IT) architecture for Certifying Authorities may support open standards and accepted de facto standards; the most important standards that may be considered for different activities associated with the Certifying Authority?s functions are as under:

The product	The standard
Public Key Infrastructure	PKIX
Digital Signature Certificates and Digital Signature revocation list	X.509. version 3 certificates as specified in ITU RFC 1422
Directory (DAP and LDAP)	X500 for publication of certificates and Certification Revocation Lists (CRLs)
Database Management Operations	Use of generic SQL
Public Key algorithm	DSA and RSA
Digital Hash Function	MD5 and SHA-1
RSA Public Key Technology	PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit) PKCS#5 Password Based Encryption Standard PKCS#7 Cryptographic Message Syntax standard PKCS#8 Private Key Information Syntax standard PKCS#9 Selected Attribute Types PKCS#10 RSA Certification Request PKCS#12 Portable format for storing/transporting a

	user?s private keys and certificates
Distinguished name	X.520
Digital Encryption and Digital Signature	PKCS#7
Digital Signature Request Format	PKCS#10

7. Digital Signature Certificate Standard.- All Digital Signature Certificates issued by the Certifying Authorities shall conform to ITU X.509 version 3 standard as per rule 6 and shall inter alia contain the following data, namely
a.Serial Number (assigning of serial number to the Digital Signature Certificate by Certifying Authority to distinguish it from other certificate)
b.Signature Algorithm Identifier (which identifies the algorithm used by Certifying Authority to sign the Digital Signature Certificate)
c.Issuer Name (name of the Certifying Authority who issued the Digital Signature Certificate)
d.Validity period of the Digital Signature Certificate
e.Name of the subscriber (whose public key the Certificate identifies); and
f.Public Key information of the subscriber.

8. Licensing of Certifying Authorities
(1) The following persons may apply for grant of a licence to issue Digital Signature Certificates, namely :-
a.an individual, being a citizen of India and having a capital of five crores of rupees or more in his business or profession
b.a company having ?
(i)paid up capital of not less than five crores of rupees; and
(ii) net worth of not less than fifty crores of rupees:
Provided that no company in which the equity share capital held in aggregate by the Non-resident Indians, Foreign Institutional Investors, or foreign companies, exceeds forty-nine per cent of its capital, shall be eligible for grant of licence:

Provided further that in a case where the company has been registered under the Companies Act, 1956
(1 of 1956) during the preceding financial year or in the financial year during which it applies for grant of
licence under the Act and whose main object is to act as Certifying Authority, the net worth referred to in
sub-clause (ii) of this clause shall be the aggregate net worth of its majority shareholders holding at least
51% of paid equity capital, being the Hindu Undivided Family, firm or company:

Provided also that the majority shareholders referred to in the second proviso shall not include Non-resident Indian, foreign national, Foreign Institutional Investor and foreign company:

Provided also that the majority shareholders of a company referred to in the second proviso whose net
worth has been determined on the basis of such majority shareholders, shall not sell or transfer its equity
shares held in such company-

(i) unless such a company acquires or has its own net worth of not less than fifty crores of rupees;
(ii) without prior approval of the Controller;
c.a firm having ?
i.capital subscribed by all partners of not less than five crores of rupees; and
ii.net worth of not less than fifty crores of rupees:

Provided that no firm, in which the capital held in aggregate by any Non-resident Indian, and foreign national, exceeds forty-nine per cent of its capital, shall be eligible for grant of licence:

Provided further that in a case where the firm has been registered under the Indian Partnership Act, 1932 (9 of 1932) during the preceding financial year or in the financial year during which it applies for grant of licence under the Act and whose main object is to act as Certifying Authority, the net worth referred to in sub-clause (ii) of this clause shall be the aggregate net worth of all of its partners:

Provided also that the partners referred to in the second proviso shall not include Non-resident Indian and foreign national:

Provided also that the partners of a firm referred to in the second proviso whose net worth has been determined on the basis of such partners, shall not sell or transfer its capital held in such firm-

(i) unless such firm has acquired or has its own net worth of not less than fifty crores of rupees;
(ii) without prior approval of the Controller;
(d) Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments.

Explanation.- For the purpose of this rule,-

i. "company" shall have the meaning assigned to it in clause 17 of section 2 of the Income-tax Act,1961 (43 of 1961);
ii. "firm", "partner" and "partnership" shall have the meanings respectively assigned to them in the Indian Partnership Act, 1932 (9 of 1932); but the expression "partner" shall also include any person who, being a minor has been admitted to the benefits of partnership;
iii. "foreign company" shall have the meaning assigned to it in clause (23A) of section 2 of the Income-tax Act,1961 (43 of 1961)
iv. "net worth" shall have the meaning assigned to it in clause (ga) of sub-section (1) of section 3 of the Sick Industrial Companies (Special Provisions) Act, 1985 (1 of 1986)
v. "Non-resident" shall have the meaning assigned to it as in clause 26 of section 2 of the Income-tax Act,1961 (43 of 1961)
(2) The applicant being an individual, or a company, or a firm under sub-rule (1), shall submit a performance bond or furnish a banker?s guarantee from a scheduled bank in favour of the Controller in such form and in such manner as may be approved by the Controller for an amount of not less than five crores of rupees and the performance bond or banker?s guarantee shall remain valid for a period of six years from the date of its submission:

Provided that the company and firm referred to in the second proviso to clause (b) and the second proviso to clause (c) of sub-rule (1) shall submit a performance bond or furnish a banker?s guarantee for ten crores of rupees:

Provided further that nothing in the first proviso shall apply to the company or firm after it has acquired or has its net worth of fifty crores of rupees.

(3) Without prejudice to any penalty which may be imposed or prosecution may be initiated for any offence under the Act or any other law for the time being in force, the performance bond or banker?s guarantee may be invoked ?

f. when the Controller has suspended the licence under sub-section (2)
of section 25 of the Act; or
g. for payment of an offer of compensation made by the Controller; or
h. for payment of liabilities and rectification costs attributed to the negligence of the Certifying Authority, its officers or employees; or

i. for payment of the costs incurred in the discontinuation or transfer of operations of the licensed Certifying Authority, if the Certifying Authority's licence or operations is discontinued; or
j. any other default made by the Certifying Authority in complying with the provisions of the Act or rules made thereunder.

Explanation.- "transfer of operation" shall have the meaning assigned to it in clause (47)
of section 2 of the Income-tax Act, 1961 (43 of 1961).

9. Location of the Facilities.-The infrastructure associated with all functions of generation, issue and management of Digital Signature Certificate as well as maintenance of Directories containing information about the status, and validity of Digital Signature Certificate shall be installed at any location in India.

10. Submission of Application.- Every application for a licensed Certifying Authority shall be made to the
Controller,-

i.in the form given at Schedule-I; and
ii.in such manner as the Controller may, from time to time, determine,supported by such documents and information as the Controller may require and it shall inter alia include-
a. a Certification Practice Statement (CPS);
b. a statement including the procedures with respect to identification of the applicant;
c. a statement for the purpose and scope of anticipated Digital Signature Certificate technology, management, or operations to be outsourced;
d. certified copies of the business registration documents of Certifying Authority that intends to be licensed;
e. a description of any event, particularly current or past insolvency, that could materially affect the applicant's ability to act as a Certifying Authority;
f. an undertaking by the applicant that to its best knowledge and belief it can and will comply with the requirements of its Certification Practice Statement;
g. an undertaking that the Certifying Authority?s operation would not commence until its operation and facilities associated with the functions of generation, issue and management of Digital Signature Certificate are audited by the auditors and approved by the Controller in accordance with rule 20;
h. an undertaking to submit a performance bond or banker?s guarantee in accordance with sub-rule (2) of rule 8 within one month of Controller indicating his approval for the grant of licence to operate as a Certifying Authority;
i. any other information required by the Controller.

12. Fee.- (1) The application for the grant of a licence shall be accompanied by a non-refundable fee of twenty-five thousand rupees payable by a bank draft or by a pay order drawn in the name of the Controller.

(2) The application submitted to the Controller for renewal of Certifying Authority?s licence shall be accompanied by a non-refundable fee of five thousand rupees payable by a bank draft or by a pay order drawn in the name of the Controller.
(3) Fee or any part thereof shall not be refunded if the licence is suspended or revoked during its validity period.

13. Cross Certification.- (1) The licensed Certifying Authority shall have arrangement for cross certification with other licensed Certifying Authorities within India which shall be submitted to the Controller before the commencement of their operations as per rule 20:

Provided that any dispute arising as a result of any such arrangement between the Certifying Authorities; or between Certifying Authorities or Certifying Authority and the Subscriber, shall be referred to the Controller for arbitration or resolution.

(2) The arrangement for Cross Certification by the licensed Certifying Authority with a Foreign Certifying Authority along with the application, shall be submitted to the Controller in such form and in such manner as may be provided in the regulations made by the Controller; and the licensed Certifying Authority shall not commence cross certification operations unless it has obtained the written or digital signature approval from the Controller.

14. Validity of licence.- (1) A licence shall be valid for a period of five years from the date of its issue.

(2) The licence shall not be transferable.

15. Suspension of Licence.- (1) The Controller may by order suspend the licence in accordance with the provisions contained in sub-section (2) of section 25 of the Act.

(2) The licence granted to the persons referred to in clauses (a) to (c) of sub-rule (1) of rule 8 shall stand suspended when the performance bond submitted or the banker?s guarantee furnished by such persons is invoked under sub-rule (2) of that rule.

16. Renewal of licence.- (1) The provisions of rule 8 to rule 13, shall apply in the case of an application for renewal of a licence as it applies to a fresh application for licensed Certifying Authority.

(2) A Certifying Authority shall submit an application for the renewal of its licence not less than forty-five days before the date of expiry of the period of validity of licence.

(3) The application for renewal of licence may be submitted in the form of electronic record subject to such requirements as the Controller may deem fit.

CERTIFYING AUTHORITIES RULES, 2000

17. Issuance of Licence.- (1) The Controller may, within four weeks from the date of receipt of the application, after considering the documents accompanying the application and such other factors, as he may deem fit, grant or renew the licence or reject the application:

Provided that in exceptional circumstances and for reasons to be recorded in writing, the period of four weeks may be extended to such period, not exceeding eight weeks in all as the Controller may deem fit.

(2) If the application for licensed Certifying Authority is approved, the applicant shall -

a.submit a performance bond or furnish a banker?s guarantee within one month from the date of such approval to the Controller in accordance with sub-rule (2) of rule 8; and

b.execute an agreement with the Controller binding himself to comply with the terms and conditions of the licence and the provisions of the Act and the rules made thereunder.

18. Refusal of Licence.- The Controller may refuse to grant or renew a licence if-

i. the applicant has not provided the Controller with such information relating to its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require; or

ii. the applicant is in the course of being wound up or liquidated; or

iii. a receiver has, or a receiver and manager have, been appointed by the court in respect of the applicant; or

iv. the applicant or any trusted person has been convicted, whether in India or out of India, of an offence the conviction for which involved a finding that it or such trusted person acted fraudulently or dishonestly, or has been convicted of an offence under the Act or these rules; or

v. the Controller has invoked performance bond or banker?s guarantee; or

vi. a Certifying Authority commits breach of, or fails to observe and comply with, the procedures and practices as per the Certification Practice Statement; or

vii. a Certifying Authority fails to conduct, or does not submit, the returns of the audit in accordance with rule 31; or

viii. the audit report recommends that the Certifying Authority is not worthy of continuing Certifying

Authority?s operation; or
ix. a Certifying Authority fails to comply with the directions of the Controller.

19.Governing Laws.- The Certification Practice Statement of the Certifying Authority shall comply with, and be governed by, the laws of the country.

20.Security Guidelines for Certifying Authorities.- (1) The Certifying Authorities shall have the sole responsibility of integrity, confidentiality and protection of information and information assets employed in its operation, considering classification, declassification, labeling, storage, access and destruction of
information assets according to their value, sensitivity and importance of operation.
(2) Information Technology Security Guidelines and Security Guidelines for Certifying Authorities aimed at protecting the integrity, confidentiality and availability of service of Certifying Authority are given in
Schedule-II and Schedule-III respectively.
(i)The Certifying Authority shall formulate its Information Technology and Security Policy for operation complying with these guidelines and submit it to the Controller before commencement of operation:
(ii)Provided that any change made by the Certifying Authority in the Information Technology and Security Policy shall be submitted by it within two weeks to the Controller.

21. Commencement of Operation by Licensed Certifying Authorities.- The licensed Certifying
Authority shall commence its commercial operation of generation and issue of Digital Signature only after -
(a) it has confirmed to the Controller the adoption of Certification Practice Statement;
(b) it has generated its key pair, namely, private and corresponding public key, and submitted the public key to the Controller;
a.the installed facilities and infrastructure associated with all functions of generation, issue and management of Digital Signature Certificate have been audited by the accredited auditor in accordance with the provisions of rule 31; and
b.it has submitted the arrangement for cross certification with other licensed Certifying Authorities within India to the Controller.

22. Requirements Prior to Cessation as Certifying Authority.- Before ceasing to act as a Certifying Authority, a Certifying Authority shall, -
(a) give notice to the Controller of its intention to cease acting as a Certifying Authority:
Provided that the notice shall be made ninety days before ceasing to act as a Certifying Authority or ninety days before the date of expiry of licence;
(b) advertise sixty days before the expiry of licence or ceasing to act as Certifying Authority, as the case may be, the intention in such daily newspaper or newspapers and in such manner as the Controller may determine;
(c) notify its intention to cease acting as a Certifying Authority to the subscriber and Cross Certifying Authority of each unrevoked or unexpired Digital Signature Certificate issued by it :

Provided that the notice shall be given sixty days before ceasing to act as a Certifying Authority or sixty days before the date of expiry of unrevoked or unexpired Digital Signature Certificate, as the case may be;
(d) the notice shall be sent to the Controller, affected subscribers and Cross Certifying Authorities by digitally signed e-mail and registered post;
(e) revoke all Digital Signature Certificates that remain unrevoked or unexpired at the end of the ninety days notice period, whether or not the subscribers have requested revocation;
(f) make a reasonable effort to ensure that discontinuing its certification services causes minimal disruption to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding Digital Signature Certificates;
(g) make reasonable arrangements for preserving the records for a period of seven years;

(h) pay reasonable restitution (not exceeding the cost involved in obtaining the new Digital Signature Certificate) to subscribers for revoking the Digital Signature Certificates before the date of expiry;
(i) after the date of expiry mentioned in the licence, the Certifying Authority shall destroy the certificate?signing private key and confirm the date and time of destruction of the private key to the Controller.

23. Database of Certifying Authorities.- The Controller shall maintain a database of the disclosure record of every Certifying Authority, Cross Certifying Authority and Foreign Certifying Authority, containing inter alia the following details:
a.the name of the person/names of the Directors, nature of business, Income-tax Permanent Account Number, web address, if any, office and residential address, location of facilities associated with functions of generation of Digital Signature Certificate, voice and facsimile telephone numbers, electronic mail address(es), administrative contacts and authorized representatives;
b.the public key(s), corresponding to the private key(s) used by the Certifying Authority and recognized foreign Certifying Authority to digitally sign Digital Signature Certificate;
c.current and past versions of Certification Practice Statement of Certifying Authority;
d.time stamps indicating the date and time of -
i.grant of licence;
ii.confirmation of adoption of Certification Practice Statement and its earlier versions by Certifying Authority;
iii.commencement of commercial operations of generation and issue of Digital Signature Certificate by the Certifying Authority;
iv.revocation or suspension of licence of Certifying Authority;
v.commencement of operation of Cross Certifying Authority;
vi.issue of recognition of foreign Certifying Authority;
vii.revocation or suspension of recognition of foreign Certifying Authority.

24. Digital Signature Certificate.- The Certifying Authority shall, for issuing the Digital Signature Certificates, while complying with the provisions of section 35 of the Act, also comply with the following, namely:-
(a) the Digital Signature Certificate shall be issued only after a Digital Signature Certificate application
in the form provided by the Certifying Authority has been submitted by the subscriber to the Certifying Authority and the same has been approved by it:

Provided that the application Form contains, inter alia, the particulars given in the modal Form given in Schedule-IV;
(b) no interim Digital Signature Certificate shall be issued;
(c) the Digital Signature Certificate shall be generated by the Certifying Authority upon receipt of an authorised and validated request for:-
(i) new Digital Signature Certificates;
(ii) Digital Signature Certificates renewal;
(d) the Digital Signature Certificate must contain or incorporate, by reference such information, as is sufficient to locate or identify one or more repositories in which revocation or suspension of the Digital Signature Certificate will be listed, if the Digital Signature Certificate is suspended or revoked;
(e) the subscriber identity verification method employed for issuance of Digital Signature Certificate shall be specified in the Certification Practice Statement and shall be subject to the approval of the Controller during the application for a licence; a.where the Digital Signature Certificate is issued to a person (referred to in this clause as a New Digital Signature Certificate) on the basis of another valid Digital Signature Certificate held by the said person (referred in this clause as an Originating Digital Signature Certificate) and subsequently the originating Digital Signature Certificate has been suspended or revoked, the Certifying Authority that issued the new Digital Signature Certificate shall conduct investigations to determine whether it is necessary to

suspend or revoke the new Digital Signature Certificate;

b.the Certifying Authority shall provide a reasonable opportunity for the subscriber to verify the contents of the Digital Signature Certificate before it is accepted;

c.if the subscriber accepts the issued Digital Signature Certificate, the Certifying Authority shall publish a signed copy of the Digital Signature Certificate in a repository;

d.where the Digital Signature Certificate has been issued by the licensed Certifying Authority and accepted by the subscriber, and the Certifying Authority comes to know of any fact, or otherwise, that affects the validity or reliability of such Digital Signature Certificate, it shall notify the same to the subscriber immediately;

e.all Digital Signature Certificates shall be issued with a designated expiry date.

25.Generation of Digital Signature Certificate.- The generation of the Digital Signature Certificate shall involve: receipt of an approved and verified Digital Signature Certificate request; creating a new Digital Signature Certificate; binding the key pair associated with the Digital Signature Certificate to a Digital Signature Certificate owner; issuing the Digital Signature Certificate and the associated public key for operational use; a distinguished name associated with the Digital Signature Certificate owner; and a recognized and relevant policy as defined in Certification Practice Statement.

26. Issue of Digital Signature Certificate.- Before the issue of the Digital Signature Certificate, the Certifying Authority shall:-

i. confirm that the user?s name does not appear in its list of compromised users;

ii. comply with the procedure as defined in his Certification Practice Statement including verification of identification and/or employment;

iii. comply with all privacy requirements;

iv. obtain a consent of the person requesting the Digital Signature Certificate, that the details of such Digital Signature Certificate can be published on a directory service.

26.Certificate Lifetime.- (1) A Digital Signature Certificate,- shall be issued with a designated expiry date; 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; shall expire automatically upon reaching the designated expiry date at which time the

(1)Digital Signature Certificate shall be archived; 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.

27. Archival of Digital Signature Certificate.- A Certifying Authority shall archive -

a.applications for issue of Digital Signature Certificates;

b.registration and verification documents of generated Digital Signature Certificates;

c.Digital Signature Certificates;

d.notices of suspension;

e.information of suspended Digital Signature Certificates;

f.information of revoked Digital Signature Certificates;

g.expired Digital Signature Certificates, for a minimum period of seven years or for a period in accordance with legal requirement.

28. Compromise of Digital Signature Certificate.- Digital Signature Certificates in operational use that become compromised shall be revoked in accordance with the procedure defined in the Certification Practice Statement of Certifying Authority.

Explanation : Digital Signature Certificates shall,-

(a) be deemed to be compromised where the integrity of:-

(i) the private key associated with the Digital Signature Certificate is in doubt;

(ii) the Digital Signature Certificate owner is in doubt, as to the use, or attempted use of his key pairs, or otherwise, for malicious or unlawful purposes;
(b) remain in the compromised state for only such time as it takes to arrange for revocation.

29. Revocation of Digital Signature Certificate.- (1) Digital Signature Certificate shall be revoked and become invalid for any trusted use, where -
a.there is a compromise of the Digital Signature Certificate owner?s private key;
b.there is a misuse of the Digital Signature Certificate;
c.there is a misrepresentation or errors in the Digital Signature Certificate;
d.the Digital Signature Certificate is no longer required.
(2) The revoked Digital Signature Certificate shall be added to the Certificate Revocation List (CRL).

30. Fees for issue of Digital Signature Certificate.- (1) The Certifying Authority shall charge such fee for the issue of Digital Signature Certificate as may be prescribed by the Central Government under sub-section (2) of section 35 of the Act.
(2) Fee may be payable in respect of access to Certifying Authority?s X.500 directory for certificate downloading. Where fees are payable, Certifying Authority shall provide an up-to-date fee schedule to all its subscribers and users, this may be done by publishing fee schedule on a nominated website.
(3) Fees may be payable in respect of access to Certifying Authority?s X.500 directory service for certificate revocation or status information. Where fees are payable, Certifying Authority shall provide an up-to-date fee schedule to all its subscribers and users, this may be done by publishing the fee schedule on a nominated website.
(4) No fee is to be levied for access to Certification Practice Statement via Internet. A fee may be charged by the Certifying Authority for providing printed copies of its Certification Practice Statement.

31. Audit.- (1) The Certifying Authority shall get its operations audited annually by an auditor and such audit shall include inter alia,-
i. security policy and planning;
ii. physical security;
iii. technology evaluation;
iv. Certifying Authority?s services administration;
v. relevant Certification Practice Statement;
vi. compliance to relevant Certification Practice Statement;
vii. contracts/agreements;
viii. regulations prescribed by the Controller;
ix. policy requirements of Certifying Authorities Rules, 2000.
(2) The Certifying Authority shall conduct,-
(a) half yearly audit of the Security Policy, physical security and planning of its operation;
(b) a quarterly audit of its repository.
(3) The Certifying Authority shall submit copy of each audit report to the Controller within four weeks of the completion of such audit and where irregularities are found, the Certifying Authority shall take immediate appropriate action to remove such irregularities.

32. Auditor?s relationship with Certifying Authority.- (1) The auditor shall be independent of the Certifying Authority being audited and shall not be a software or hardware vendor which is, or has been providing services or supplying equipment to the said Certifying Authority.

(2) The auditor and the Certifying Authority shall not have any current or planned financial, legal or other relationship, other than that of an auditor and the audited party.

33.Confidential Information.- The following information shall be confidential namely:--
a.Digital Signature Certificate application, whether approved or rejected;
b.Digital Signature Certificate information collected from the subscriber or elsewhere as part of

the registration and verification record but not included in the Digital Signature Certificate information;
c.subscriber agreement.

34. Access to Confidential Information.- (1) Access to confidential information by Certifying Authority?s operational staff shall be on a "need-to-know" and "need-to-use" basis.
(2) Paper based records, documentation and backup data containing all confidential information as prescribed in rule 33 shall be kept in secure and locked container or filing system, separately from all other records.
(3) The confidential information shall not be taken out of the country except in a case where a properly constitutional warrant or other legally enforceable document is produced to the Controller and he permits to do so.

CERTIFYING AUTHORITIES RULES, 2000

SCHEDULE-I

[See rule 10]

Form for Application for grant of Licence to be a Certifying Authority

For Individual

1. Full Name *

Last Name/Surname ______________________________
First Name _______________________________
Middle Name _______________________________

2. Have you ever been known by any other name? If Yes,

Last Name/Surname ______________________________
First Name _______________________________
Middle Name _______________________________

3. Address

A. Residential Address *

Flat/Door/Block No. _______________________________
Name of Premises/Building/Village _______________________________
Road/Street/Lane/Post Office _______________________________
Area/Locality/Taluka/Sub-Division _______________________________
Town/City/District _______________________________
State/Union Territory ________________ Pin : _________ Telephone No.
____
Fax _______________________________
Mobile Phone No. _______________________________

B. Office Address *

Name of Office _______________________________
Flat/Door/Block No. _______________________________
Name of Premises/Building/Village _______________________________
Road/Street/Lane/Post Office _______________________________
Area/Locality/Taluka/Sub-Division _______________________________
Town/City/District _______________________________
State/Union Territory ________________ Pin : _________
Telephone No. _______________________________

Fax ___________________________________

4. Address for Communication * Tick ˚as applicable A or B

5. Father?s Name *

Last Name/Surname ___________________________________
First Name ___________________________________
Middle Name ___________________________________

6. Sex * (For Individual Applicant only) Tick ˚as applicable : Male / Female

7. Date of Birth (dd/mm/yyyy) * --/--/----

8. Nationality * ___________________________________

9. Credit Card Details

Credit Card Type ___________________________________
Credit Card No. ___________________________________
Issued By ___________________________________

10. E-mail Address ___________________________________

11. Web URL address ___________________________________

12. Passport Details #

Passport No. ___________________________________
Passport issuing authority ___________________________________
Passport expiry date (dd/mm/yyyy) --/--/----

13. Voter?s Identity Card No. # ___________________________________

14. Income Tax PAN no. # ___________________________________

15. ISP Details

ISP Name * ___________________________________
ISP?s Website Address, if any ___________________________________
Your User Name at ISP, if any ___________________________________

16. Personal Web page URL address, if any ___________________________________

17. Capital in the business or profession * Rs. ________________________________(Attach documentary proof)

For Company /Firm/Body of Individuals/Association of Persons/ Local Authority

18. Registration Number * ___________________________________

19. Date of Incorporation/Agreement/Partnership * --/--/----

20. Particulars of Business, if any: *

Head Office ___________________________________

Name of Office ___________________________________
Flat/Door/Block No. _______________________________
Name of Premises/Building/Village _____________________________________
Road/Street/Lane/Post Office _____________________________________
Area/Locality/Taluka/Sub-Division _____________________________________
Town/City/District _______________________ Pin _________
State/Union Territory _____________________________________
Telephone No. _____________________________________
Fax _____________________________________
Web page URL address, if any _____________________________________
No. of Branches _____________________________________
Nature of Business _____________________________________

21. Income Tax PAN No.* _____________________________________

22. Turnover in the last financial year Rs. _________________________________

23. Net worth * Rs. _________________________________(Attach documentary proof)

24. Paid up Capital * Rs. _________________________________(Attach documentary proof)

25. Insurance Details

Insurance Policy No.* _____________________________________
Insurer Company * _____________________________________

26. Names, Addresses etc. of Partners/Members/Directors (For Information about more persons,please add separate sheet(s) in the format given in the next page) *

No. of Partners/Members/Directors _____________________________________ Details of Partners/Members/Directors

A. Full Name

Last Name/Surname ____________________________________
First Name _____________________________________
Middle Name _____________________________________

B. Address

Flat/Door/Block No. _________________________________
Name of Premises/Building/Village _________________________________
Road/Street/Lane/Post Office _________________________________
Area/Locality/Taluka/Sub-Division _________________________________
Town/City/District _________________________________
State/Union Territory Pin _________________________________
Telephone No. _________________________________
Fax No. _________________________________
Mobile Phone No. _________________________________

C. Nationality _________________________________In case of foreign national, Visa details_________________________________

D. Passport Details #

Passport No. _____________________________________

Passport issuing authority ___________________________________
Passport expiry date ___________________________________

E. Voter?s Identity Card No. # ___________________________________

F. Income Tax PAN no. # ___________________________________

G. E-mail Address ___________________________________

H. Personal Web page URL, if any ___________________________________

27. Authorised Representative *

Name ___________________________________
Flat/Door/Block No. ___________________________________
Name of Premises/Building/Village ___________________________________
Road/Street/Lane/Post Office ___________________________________
Area/Locality/Taluka/Sub-Division ________________________________
Town/City/District ___________________ Pin ____________
State/Union Territory ___________________________________
Telephone No. ___________________________________
Fax ___________________________________
Nature of Business ___________________________________

For Government Ministry/Department/Agency/Authority

28. Particulars of Organisation: *

Name of Organisation ___________________________________
Administrative Ministry/Department ___________________________________
Under State/Central Government ___________________________________
Flat/Door/Block No. ___________________________________
Name of Premises/Building/Village ___________________________________
Road/Street/Lane/Post Office ___________________________________
Area/Locality/Taluka/Sub-Division ___________________________________
Town/City/District ____________________ Pin __________
State/Union Territory ___________________________________
Telephone No. ___________________________________
Fax No. ___________________________________
Web page URL Address ___________________________________
Name of the Head of Organisation ___________________________________
Designation ___________________________________
E-mail Address ___________________________________

29. Bank Details

Bank Name * ___________________________________
Branch * ___________________________________
Bank Account No. * ___________________________________
Type of Bank Account * ___________________________________

30. Whether bank draft/pay order for licence fee enclosed * : Y / N If yes,

Name of Bank ________________________________
Draft/pay order No. ________________________________
Date of Issue ________________________________

Amount ________________________________

31. Location of facility in India for generation of Digital Signature Certificate *
____

32. Public Key @ ________________________________

33. Whether undertaking for Bank Guarantee/Performance Bond attached * : Y / N (Not applicable if the applicant is a Government Ministry/Department/Agency/ Authority)

34. Whether Certification Practice Statement is enclosed * : Y / N

35. Whether certified copies of business registration document are enclosed : Y / N (For Company/ Firm/ Body of Individuals/ Association of Persons/ Local Authority) If yes, the documents attached:

i.??????????
ii.??????????
iii.??????????

36. Any other information
____Date
Signature of the Applicant
____

Instructions :
1. Columns marked with * are mandatory.
2. For the columns marked with #, details for at least one is mandatory.
3. Column No. 1 to 17 are to be filled up by individual applicant.
1.Column No. 18 to 27 are to be filled up if applicant is a Company/ Firm/ Body of Individuals/Association of Persons/ Local Authority.
2.Column No. 28 is to be filled up if applicant is a Government organisation.
3.Column No. , 29, 30, 31 and 34 are to be filled up by all applicants.
4.@ Column No. 32 is applicable only for application for renewal of licence.
5.Column No. 33 is not applicable if the applicant is a Government organisation.

SCHEDULE-II

[See rule 19(2)]

Information Technology (IT) Security Guidelines

Index

Page

Information Technology (IT) Security Guidelines

1. Introduction

This document provides guidelines for the implementation and management of Information Technology Security. Due to the inherent dynamism of the security requirements, this document does not provide an exact template for the organizations to follow. However, appropriate suitable samples of security process are provided for guidelines. It is the responsibility of the organizations to develop internal processes that meet the guidelines set forth in this document.The following words used in the Information Technology Security Guidelines shall be interpreted as follows:

shall: The guideline defined is a mandatory requirement, and therefore must be complied with.

should: The guideline defined is a recommended requirement. Non-compliance shall be documented and approved by the management. Where appropriate, compensating controls shall be implemented.

must: The guideline defined is a mandatory requirement, and therefore must be complied with.

may: The guideline defined is an optional requirement. The implementation of this guideline is determined by the organisation?s requirement.

2. Implementation of an Information Security Programme

Successful implementation of a meaningful Information Security Programme rests with the support of the top management. Until and unless the senior managers of the organization understand and concur with the objectives of the information security programme its ultimate

success is in question.
The Information Security Programme should be broken down into specific stages as follows:

a.Adoption of a security policy;
b.Security risk analysis;
c.Development and implementation of a information classification system;
d.Development and implementation of the security standards manual;
e.Implementation of the management security self-assessment process;
f.On-going security programme maintenance and enforcement; and
g.Training.

The principal task of the security implementation is to define the responsibilities of persons within the organization. The implementation should be based on the general principle that the person who is generating the information is also responsible for its security. However, in order to enable him to carry out his responsibilities in this regard, proper tools, and environment need to be established. When different pieces of information at one level are integrated to form higher value information, the responsibility for its security needs also should go up in the hierarchy to the integrator and should require higher level of authority for its access. It should be absolutely clear with respect to each information as to who is its owner, its custodian, and its users. It is the duty of the owner to assign the right classification to the information so that the required level of security can be enforced. The custodian of information is responsible for the proper implementation of security guidelines and making the information available to the users on a need to know basis.

CERTIFYING AUTHORITIES RULES, 2000

3. Information Classification

Information assets must be classified according to their sensitivity and their importance to the organization. Since it is unrealistic to expect managers and employees to maintain absolute control over all information within the boundaries of the organization, it is necessary to advise them on which types of information are considered more sensitive, and how the organization would like the sensitive information handled and protected. Classification, declassification, labeling, storage, access, destruction and reproduction of classified data and the administrative overhead this process will create must be considered. Failure to maintain a balance between the value of the information classified and the administrative burden the classification system places on the organization will result in long-term difficulties in achieving success. Confidential is that classification of information of which unauthorized disclosure/use could cause serious damage to the organization, e.g. strategic planning documents.
Restricted is that classification of information of which unauthorized disclosure/use would not be in the best interest of the organization and/or its customers, e.g. design details, computer software (programs, utilities), documentation, organization personnel data, budget information .Internal use is that classification of information that does not require any degree of protection against disclosure within the company, e.g. operating procedures, policies and standards inter office memorandums.

Unclassified is that classification of information that requires no protection against disclosure e.g. published annual reports, periodicals.

While the above classifications are appropriate for a general organization view point, the following classifications may be considered :

Top Secret: It shall be applied to information unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for Nation?s closest secrets and to be used with great reserve.

Secret: This shall be applied to information unauthorized disclosure of which could be expected to cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information and is the highest classification normally used.

Confidentiality: This shall be applied to information unauthorized disclosure of which could be expected to cause damage to the security of the organisation or could be prejudicial to the interest of the organisation, or could affect the organisation in its functioning. Most information will on proper analysis be classified no higher than confidential.

Restricted: This shall be applied to information which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose.

Unclassified: This is the classification of information that requires no protection against disclosure.

4. Physical and Operational Security

4.1 Site Design
1.The site shall not be in locations that are prone to natural or man-made disasters, like flood, fire, chemical contamination and explosions.
2.As per nature of the operations, suitable floor structuring, lighting, power and water damage protection requirements shall be provided.
3.Construction shall comply with all applicable building and safety regulations as laid down by the relevant Government agencies. Further, the construction must be tamper-evident.
4.Materials used for the construction of the operational site shall be fire-resistant and free of toxic chemicals.
5.External walls shall be constructed of brick or reinforced concrete of sufficient thickness to resist forcible attack. Ground level windows shall be fortified with sturdy mild steel grills or impact-resistant laminated security glass. All internal walls must be from the floor to the ceiling and must be tamper-evident.
6.Air-conditioning system, power supply system and uninterrupted power supply unit with proper backup shall be installed depending upon the nature of operation. All ducting holes of the air-conditioning system must be designed so as to prevent intrusion of any kind.
7.Automatic fire detection, fire suppression systems and equipment in compliance with requirement specified by the Fire Brigade or any other agencies of the Central or State Government shall be installed at the operational site.
8.Media library, electrical and mechanical control rooms shall be housed in separate isolated areas, with access granted only to specific, named individuals on a need basis.
9.Any facility that supports mission-critical and sensitive applications must be located and designed for repairability, relocation and reconfiguration. The ability to relocate, reconstitute and reconfigure these applications must be tested as part of the business continuity/ disaster recovery plan.

4.2 Fire Protection

1.Combustible materials shall not be stored within hundred meters of the operational site.
2.Automatic fire detection, fire suppression systems and audible alarms as prescribed by the Fire Brigade or any other agency of the Central or State Government shall be installed at the operational site.
3.Fire extinguishers shall be installed at the operational site and their locations clearly marked with appropriate signs.
4.Periodic testing, inspection and maintenance of the fire equipment and fire suppression systems shall be carried out.
5.Procedures for the safe evacuation of personnel in an emergency shall be visibly pasted/displayed at prominent places at the operational site. Periodic training and fire drills shall

be conducted.
6.There shall be no eating, drinking or smoking in the operational site. The work areas shall be kept clean at all times.

4.3 Environmental Protection

1.Water detectors shall be installed under the raised floors throughout the operational site and shall be connected to audible alarms.
2.The temperature and humidity condition in the operational site shall be monitored and controlled periodically.
3.Personnel at the operational site shall be trained to monitor and control the various equipment and devices installed at the operational site for the purpose of fire and environment protection.
4.Periodic inspection, testing and maintenance of the equipment and systems shall be scheduled.

4.4 Physical Access

1.Responsibilities round the clock, seven days a week, three hundred sixty five days a year for physical security of the systems used for operation and also actual physical layout at the site of operation shall be defined and assigned to named individuals.
2.Biometric physical access security systems shall be installed to control and audit access to the operational site.
3.Physical access to the operational site at all times shall be controlled and restricted to authorised personnel only. Personnel authorized for limited physical access shall not be allowed to gain unauthorized access to restricted area within operational site.
4.Dual control over the inventory and issue of access cards/keys during normal business hours to the Data Centre shall be in place. An up-to-date list of personnel who possess the cards/keys shall be regularly maintained and archived for a period of three years.
5.Loss of access cards/keys must be immediately reported to the security supervisor of the operational site who shall take appropriate action to prevent unauthorised access.
6.All individuals, other than operations staff, shall sign in and sign out of the operational site and shall be accompanied by operations staff.
7.Emergency exits shall be tested periodically to ensure that the access security systems are operational.
8.All opening of the Data Centre should be monitored round the clock by surveillance video cameras.

5. Information Management

5.1 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.Organisations 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.

5.2 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.

5.3 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.

5.4 Third Party Access

1.Access to the computer systems by other organisations 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.

5.5 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 organisation. 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.

1.All incidents related to breaches shall be reported to the System Administrator or System Security Administrator for appropriate action to prevent future occurrence.
2.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.

6. System integrity and security measures

6.1 Use of Security Systems or Facilities

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

6.2 System Access Control

1.Access control software and system software security features shall be implemented to protect resources. Management approval is required to authorise 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 programme 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 authorisations 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 unauthorised disclosure and modification.
8.Stored passwords shall be protected by access controls from unauthorised 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 unauthorised 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.

6.3 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.

1.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.
2.Passwords which are easy-to-guess (e.g. user name, birth date, month, standard words etc.) should be avoided.
3.Initial or reset passwords must be changed by the user upon first use.
4.Passwords shall always be encrypted in storage to prevent unauthorized disclosure.
5.All passwords used must be resistant to dictionary attacks and all known password cracking algorithms.

6.4 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.

6.5 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 authorised 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 organisation 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.

1.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.

6.6 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, programme) 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.

7. 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 organisations shall be prohibited or strictly controlled.
3.For sensitive data, encryption of data in storage shall be considered to protect its confidentiality and integrity.

8. Data Centre Operations Security

8.1 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.

8.2 System Operations Procedure

1.Procedures shall be established to ensure that only authorised 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.

8.3 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 authorised 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 authorised 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 authorised 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.

8.4 Media Movement
1.Proper records of all movements of computer tapes/disks between on-site 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.

9. 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 programmes
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.

10. Audit Trails and Verification

1.Transactions that meet exception criteria shall be completely and accurately highlighted and reviewed by personnel independent of those that initiate the transaction.

2.Adequate audit trails shall be captured and certain information needed to determine sensitive events and pattern analysis that would indicate possible fraudulent use of the system (e.g. repeated unsuccessful logons, access attempts over a series of days) shall be analyzed. This information includes such information as who, what, when, where, and any special information such as:
i. Success or failure of the event
ii. Use of authentication keys, where applicable

1.Automated or manual procedures shall be used to monitor and promptly report all significant security events, such as accesses, which are out-of-pattern relative to time, volume, frequency,

type of information asset, and redundancy. Other areas of analysis include:
(i) Significant computer system events (e.g. configuration updates, system crashes)
(ii) Security profile changes
(iii) Actions taken by computer operations, system administrators, system programmers, and/or security administrators

2.The real time clock of the computer system shall be set accurately to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.
3.The real time clock of the computer or communications device shall be set to Indian Standard Time (IST). Further there shall be a procedure that checks and corrects drift in the real time clock.
4.Computer system access records shall be kept for a minimum of two years, in either hard copy or electronic form. Records, which are of legal nature and necessary for any legal or regulation requirement or investigation of criminal behaviour, shall be retained as per laws of the land.
5.Computer records of applications transactions and significant events must be retained for a minimum period of two years or longer depending on specific record retention requirements.

11. 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, PKI 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 alia 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.

12. 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.

13. 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.Organisation 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.Organisation 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 organisation.
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.

14. 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 organisation 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.