

<b>IT RULES under The IT Act,2000 (with Latest April,2011 Rules)</b>	<b>Page</b>
Information Technology (Certifying Authorities) Rules, 2000.	2
Information Technology (IT) Security Guidelines Rule 19 (2)	15
Security Guidelines For Certifying Authorities Rule 19 (2)	28
Form For Application For Issue Of Digital Signature Certificate Rule 23	35
The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000	38
Information Technology (Certifying Authority) Regulations, 2001	45
Cyber Regulations Appellate Tribunal (Procedure For Investigation Of Misbehaviour or Incapacity Of Presiding Officer) Rules, 2003	57
Information Technology (Other Powers Of Civil Court Vested In Cyber Appellate Tribunal) Rules 2003	59
Information Technology (Other Standards) Rules, 2003.	59
The Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003	60
The Cyber Regulations Appellate Tribunal (Salary, Allowance and other Terms and Conditions of Service of Presiding Officer) Rules, 2003.	63
Information Technology (Use Of Electronic Records And Digital Signatures) Rules, 2004	65
The Information Technology (Security Procedure) Rules, 2004	66
Blocking Of Websites Ministry Of Communication And Information Technology	67
The Cyber Appellate Tribunal (Salary, Allowance and other Term and Condition of Service of Chairperson and Members Rules, 2009	69
The Cyber Appellate Tribunal (Procedure for Investigation of Misbehavior in Capacity of Chairperson and Members) Rules, 2009	72
The Information Technology (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009	74
The Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) Rules, 2009	79
The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009	83
The Information Technology (Electronic Service Delivery) Rules, 2011	87
The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011	89
The Information Technology (Intermediaries guidelines) Rules, 2011	92
The Information Technology (Guidelines for Cyber Cafe) Rules, 2011	94

## **INFORMATION TECHNOLOGY (CERTIFYING AUTHORITIES) RULES, 2000**

### **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 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 recognised 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 utilised 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 Certification Revocation Lists (CRLs)
Database Management Operations	Use of generic SQL
Public Key algorithm	DSA and RSA
Digital Hash Function	SHA-1 and SHA-2
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 license 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 fifty lakhs of rupees and the performance bond in the form of 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 –

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

## 11. 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.

### **12. 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.

### **13. 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.

### **14. 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.

### **15. 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.

### **16. 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) furnish a performance bond in the form of 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) give an undertaking to 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.

### **17. 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.

### **18. Governing Laws.-**

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

### **19. 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.

(3) 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:

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.

### **20. 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;
- (c) 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
- (d) it has submitted the arrangement for cross certification with other licensed Certifying Authorities within India to the Controller.

### **21. 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.

## 22. 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 addresses, administrative contacts and authorised representatives;
- (b) the public key(s), corresponding to the private key(s) used by the Certifying Authority and recognised 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.

## 23. 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;
- (f) 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;
- (g) the Certifying Authority shall provide a reasonable opportunity for the subscriber to verify the contents of the Digital Signature Certificate before it is accepted;
- (h) 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;

- (i) 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;
- (j) all Digital Signature Certificates shall be issued with a designated expiry date.

#### **24. Generation of Digital Signature Certificate.-**

The generation of the Digital Signature Certificate shall involve:

- (a) receipt of an approved and verified Digital Signature Certificate request;
- (b) creating a new Digital Signature Certificate;
- (c) binding the key pair associated with the Digital Signature Certificate to a Digital Signature Certificate owner;
- (d) issuing the Digital Signature Certificate and the associated public key for operational use;
- (e) a distinguished name associated with the Digital Signature Certificate owner; and
- (f) a recognised and relevant policy as defined in Certification Practice Statement.

#### **25. 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,-

- (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.

#### **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 half yearly audit of the Security Policy, physical security and planning of its operations and the 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.

**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) \_\_\_\_\_

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.
4. Column No. 18 to 27 are to be filled up if applicant is a Company/ Firm/ Body of Individuals / Association of Persons / Local Authority.
5. Column No. 28 is to be filled up if applicant is a Government organisation.
6. Column No., 29, 30, 31 and 34 are to be filled up by all applicants.
7. @ Column No. 32 is applicable only for application for renewal of licence.
8. Column No. 33 is not applicable if the applicant is a Government organisation.

**SCHEDULE II**  
**See rule 19 (2)**  
**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. Noncompliance 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.

**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 unauthorised disclosure/use could cause serious damage to the organization, e.g. strategic planning documents.

**Restricted** is that classification of information of which unauthorised 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 unauthorised 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 unauthorised 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 unauthorised 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 manmade 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 reparability, 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 authorised for limited physical access shall not be allowed to gain unauthorised 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 authorised 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 authorise privileged access to users only on a need-to-know and need-to-do basis and also only after the authorisation 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 unauthorised 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 authorisation 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.

(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.

## **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.

(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 unauthorised disclosure.

(6) 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 authorisation 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.

(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.

## **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 welltrained 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 authorised 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 onsite and off-site media library must be maintained.

(2) There shall be procedures to ensure the authorised 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 analysed. 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

(3) 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.

(4) 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.

(5) 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.

(6) 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.

(7) 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) Authorisation, 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 authorised 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 unauthorised software must not be used on any computer, computer network or data communication equipment. In the event that any illegally acquired or unauthorised software is detected by the System Administrator or Network Administrator, the same must be removed immediately.

#### **15. 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 authorised 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 programmes 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.

#### **16. 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 authorised party prior to issue.

(3) Access to application software documentation and sensitive system software documentation shall be restricted to authorised 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) Organisations shall adopt a clean desk policy for papers, diskettes and other documentation in order to reduce the risks of unauthorised access, loss of and damage to information outside normal working hours.

#### **17. 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 authorisation 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 authorised individuals only in accordance with para 4.4 pertaining to "Physical Access".

(5) Communication and network systems shall be controlled and restricted to authorised 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 electro magnetic transmission. In this regard, use of Optical Fibre Cable and armoured 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.

#### **18. Firewalls.-**

(1) Intelligent devices generally known as "Firewalls" shall be used to isolate organisation's data network with the external network. Firewall device should also be used to limit network connectivity for unauthorised 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.

#### **19. Connectivity.-**

(1) Organisation shall establish procedure for allowing connectivity of their computer network or computer system to non-organisation 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 organisation'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 organisation'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.

## **20. 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., unauthorised 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 minimised.

(5) Only authorised 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.

## **21. Change Management-**

### **21.1 Change Control.-**

(1) Procedures for tracking and managing changes in application software, system software, hardware and data in the production system shall be established. Organisational responsibilities for the change management process shall be defined and assigned.

(2) A risk and impact analysis, classification and prioritization process shall be established.

(3) No changes to a production system shall be implemented until such changes have been formally authorised. Authorisation procedures for change control shall be defined and documented.

(4) Owners/Users shall be notified of all changes made to production system which may affect the processing of information on the said production system.

(5) Fall-back procedures in the event of a failure in the implementation of the change process shall be established and documented.

(6) Procedures to protect, control access and changes to production source code, data, execution statements and relevant system documentation shall be documented and implemented.

(7) Version changes of application software and all system software installed on the computer systems and all communication devices shall be documented. Different versions of application software and system software must be kept in safe custody.

### **21.2 Testing Of Changes To Production System.-**

(1) All changes in computer resource proposed in the production system shall be tested and the test results shall be reviewed and accepted by all concerned parties prior to implementation.

(2) All user acceptance tests in respect of changes in computer resource in production system shall be performed in a controlled environment which includes:

- (i) Test objectives,
- (ii) A documented test plan, and
- (iii) acceptance criteria.

### **21.3 Review Of Changes.-**

(1) Procedures shall be established for an independent review of programme changes before they are moved into a production environment to detect unauthorised or malicious codes.

(2) Procedures shall be established to schedule and review the implementation of the changes in computer resource in the production system so as to ensure proper functioning.

(3) All emergency changes/fixes in computer resource in the production system shall be reviewed and approved.

(4) Periodic management reports on the status of the changes implemented in the computer resource in the production system shall be submitted for management review.

## **22. Problem Management and Reporting.-**

(1) Procedures for identifying, reporting and resolving problems, such as non-functioning of Certifying Authority's system; breaches in Information Technology security; and hacking, shall be established and communicated to all personnel concerned. It shall include emergency procedures. Periodic reports shall be submitted for management review.

(2) A help desk shall be set up to assist users in the resolution of problems.

(3) A system for recording, tracking and reporting the status of reported problems shall be established to ensure that they are promptly managed and resolved with minimal impact on the user of the computing resources.

## **23. Emergency Preparedness.-**

(1) Emergency response procedures for all activities connected with computer operation shall be developed and documented. These procedures should be reviewed periodically.

(2) Emergency drills should be held periodically to ensure that the documented emergency procedures are effective.

## **24. Contingency Recovery Equipment and Services.-**

(1) Commitment shall be obtained in writing from computer equipment and supplies vendors to replace critical equipment and supplies within a specified period of time following a destruction of the computing facility.

(2) The business continuity plan shall be developed which *inter alia* include the procedures for emergency ordering of the equipment and availability of the services.

(3) The need for backup hardware and other peripherals should be evaluated in accordance to business needs.

## **25. Security Incident Reporting and Response.-**

(1) All security related incidents must be reported to a central coordinator, appointed by the management to coordinate and handle security related incidents. This central coordinator shall be the single point of contact at the organization.

(2) All incidents reported, actions taken, follow-up actions, and other related information shall be documented.

(3) Procedures shall be defined for dealing with all security related incidents, including malicious software, break-ins from networks, software bugs which compromised the security of the system.

## **26. Disaster Recovery/Management.-**

(1) Disaster recovery plan shall be developed, properly documented, tested and maintained to ensure that in the event of a failure of the information system or destruction of the facility, essential level of service will be provided. The disaster recovery framework should include:-

(a) emergency procedures, describing the immediate action to be taken in case of a major incident;

(b) fall back procedure, describing the actions to be taken to relocate essential activities or support services to a backup site;

(c) restoration procedures, describing the action to be taken to return to normal operation at the original site;

(2) The documentation should include:

(a) definition of a disaster;

(b) condition for activating the plan;

(c) stages of a crisis;

(d) who will make decisions in the crisis;

(e) role of individuals for each component of the plan;

(f) composition of the recovery team; and

(g) decision making process for return to normal operation.

(3) Specific disaster management plan for critical applications shall be developed, documented, tested and maintained on a regular basis.

(4) Responsibilities and reporting structure shall be clearly defined which will take effect immediately on the declaration of a disaster.

- (5) Each component/aspect of the plan should have a person and a backup assigned to its execution.
- (6) Periodic training of personnel and users associated with computer system and network should be conducted defining their roles and responsibilities in the event of a disaster.
- (7) Test plan shall be developed, documented and maintained. Periodic tests shall be carried out to test the effectiveness of the procedures in the plan. The results of the tests shall be documented for management review.
- (8) Disaster recovery plan should be updated regularly to ensure its continuing effectiveness.

**SCHEDULE-III**  
**[SEE RULE 19 (2)]**  
**SECURITY GUIDELINES FOR CERTIFYING AUTHORITIES**

**1. Introduction.-**

This document prescribes security guidelines for the management and operation of Certifying Authorities (CAs) and is aimed at protecting the integrity, confidentiality and availability of their services, data and systems. These guidelines apply to Certifying Authorities that perform all the functions associated with generation, issue and management of Digital Signature Certificate such as:

- (1) Verification of registration, suspension and revocation request;
- (2) Generation, issuance, suspension and revocation of Digital Signature Certificates; and
- (3) Publication and archival of Digital Signature Certificates, suspension and revocation of information.

**2. Security Management.-**

The Certifying Authority shall define Information Technology security policies for its operation on the lines defined in Schedule-II and Schedule-III. The policy shall be communicated to all personnel and widely published throughout the organisation to ensure that the personnel follow the policies.

**3. Physical controls – site location, construction and physical access.-**

(1) The site location, design, construction and physical security of the operational site of Certifying Authority shall be in accordance with para 4 of the Information Technology Security Guidelines given at Schedule-II.

(2) Physical access to the operational site housing computer servers, PKI server, communications and network devices shall be controlled and restricted to the authorised individuals only in accordance with para 4.4 of the Information Technology Security Guidelines given at Schedule-II.

(3) A Certifying Authority must:-

- (i) ensure that the operational site housing PKI servers, communications and networks is protected with fire suppression system in accordance with para 4.2 of the Information Technology Security Guidelines given at Schedule-II.
- (ii) ensure that power and air-conditioning facilities are installed in accordance with para 4.1 of the Information Technology Security Guidelines given at Schedule-II.
- (iii) ensure that all removable media and papers containing sensitive or plain text information are listed, documented and stored in a container properly identified.
- (iv) ensure unescorted access to Certifying Authority's server is limited to those personnel identified on an access list.
- (v) ensure that the exact location of Digital Signature Certification System shall not be publicly identified.
- (vi) ensure that access security system is installed to control and audit access to the Digital Signature Certification System.
- (vii) ensure that dual control over the inventory and access cards/keys are in place.
- (viii) ensure that up-to-date list of personnel who possess the access cards/keys is maintained at the Certifying Authority's operational site. Loss of access cards/keys shall be reported immediately to the Security Administrator; who shall take appropriate actions to prevent unauthorised access.
- (ix) ensure personnel not on the access list are properly escorted and supervised.
- (x) ensure a site access log is maintained at the Certifying Authority's operational site and inspected periodically.

(4) Multi-tiered access mechanism must be installed at the Certifying Authority's operational site. The facility should have clearly laid out security zones within its facility with well-defined access rights to each security zone. Each security zone must be separated from the other by floor to ceiling concrete reinforced walls. Alarm and intrusion detection system must be installed at every stage with adequate power backup capable of continuing operation even in the event of loss of main power. Electrical/Electronic circuits to external security alarm monitoring service (if used)

must be supervised. No single person must have complete access to PKI Server, root keys or any computer system or network device on his/her own.

(5) Entrance to the main building where the Certifying Authority's facilities such as Data Centre, PKI Server and Network devices are housed and entrance to each security zone must be video recorded round the clock. The recording should be carefully scrutinised and maintained for at least one year.

(6) A Certifying Authority site must be manually or electronically monitored for unauthorised intrusion at all times in accordance with the Information Technology Security Guidelines given at Schedule-II.

(7) Computer System/PKI Server performing Digital Signature Certification function shall be located in a dedicated room or partition to facilitate enforcement of physical access control. The entry and exit of the said room or partition shall be automatically locked with time stamps and shall be reviewed daily by the Security Administrator.

(8) Access to infrastructure components essential to operation of Certifying Authority such as power control panels, communication infrastructure, Digital Signature Certification system, cabling, etc. shall be restricted to authorised personnel.

(9) By-pass or deactivation of normal physical security arrangements shall be authorised and documented by security personnel.

(10) Intrusion detection systems shall be used to monitor and record physical access to the Digital Signature Certification system during and after office hours.

(11) Computer System or PKI Server performing the Digital Signature Certification functions shall be dedicated to those functions and should not be used for any other purposes.

(12) System software shall be verified for integrity in accordance with para 15 of the Information Technology Security Guidelines given at Schedule-II.

#### **4. Media Storage.-**

A Certifying Authority must ensure that storage media used by his system are protected from environment threats such as temperature, humidity and magnetic and are transported and managed in accordance with para 8.3 and para 8.4 of the Information Technology Security Guidelines given at Schedule-II.

#### **5. Waste Disposal.-**

All media used for storage of information pertaining to all functions associated with generation, production, issue and management of Digital Signature Certificate shall be scrutinised before being destroyed or released for disposal.

#### **6. Off-site Backup.-**

A Certifying Authority must ensure that facility used for off-site backup, if any, shall be within the country and shall have the same level of security as the primary Certifying Authority site.

#### **7. Change and Configuration Management.-**

(1) The components of the Certifying Authority infrastructure (e.g. cryptographic algorithm and its key parameters, operating system, system software, computer system, PKI server, firewalls, physical security, system security etc.) shall be reviewed every year for new technology risks and appropriate action plan shall be developed to manage the risks identified for each component.

(2) The application software, system software and hardware, which are procured from questionable sources, shall not be installed and used for any function associated with generation and management of Digital Signature Certificate.

(3) Software updates and patches shall be reviewed for security implications before being implemented on Certifying Authority's system.

(4) Software updates and patches to rectify security vulnerability in critical systems used for Certifying Authority's operation shall be promptly reviewed and implemented.

(5) Information on the software updates and patches and their implementation on Certifying Authority's system shall be clearly and properly documented.

#### **8. Network and Communications Security.-**

(1) Certifying Authority's systems shall be protected to ensure network access control to critical systems and services from other systems in accordance with para 17, para 18, para 19 and para 20 of the Information Technology Security Guidelines given at Schedule-II.

(2) Network connections from the Certifying Authority's system to external networks shall be restricted to only those connections which are essential to facilitate Certifying Authority's functional processes and services. Such network connections to the external network shall be properly secured and monitored regularly.

(3) Network connections should be initiated by the systems performing the functions of generation and management of Digital Signature Certificate to connect those systems performing the registration and repository functions but not *vice versa*. If this is not possible, compensating controls (e.g. use of proxy servers) shall be implemented to protect the systems performing the function of generation and management of Digital Signature Certificate from potential attacks.

(4) Systems performing the Digital Signature Certification function should be isolated to minimise their exposure to attempts to compromise the confidentiality, integrity and availability of the certification function.

(5) Communication between the Certifying Authority systems connected on a network shall be secure to ensure confidentiality and integrity of the information. For example, communications between the Certifying Authority's systems connected on a network should be encrypted and digitally signed.

(6) Intrusion detection tools should be deployed to monitor critical networks and perimeter networks and alert administrators of network intrusions and penetration attempts in a timely manner.

## 9. System Security Audit Procedures.

### 9.1 Types of event recorded.-

(1) The Certifying Authority shall maintain record of all events relating to the security of his system. The records should be maintained in audit log file and shall include such events as:-

- (i) System start-up and shutdown;
- (ii) Certifying Authority's application start-up and shutdown;
- (iii) Attempts to create, remove, set passwords or change the system privileges of the PKI Master Officer, PKI Officer, or PKI Administrator;
- (iv) Changes to keys of the Certifying Authority or any of his other details;
- (v) Changes to Digital Signature Certificate creation policies, e.g. validity period;
- (vi) Login and logoff attempts;
- (vii) Unauthorised attempts at network access to the Certifying Authority's system;
- (viii) Unauthorised attempts to access system files;
- (ix) Generation of own keys;
- (x) Creation and revocation of Digital Signature Certificates;
- (xi) Attempts to initialize remove, enable, and disable subscribers, and update and recover their keys;
- (xii) Failed read-and-write operations on the Digital Signature Certificate and Certificate Revocation List (CRL) directory.

#### (2) Monitoring and Audit Logs

- (i) A Certifying Authority should consider the use of automated security management and monitoring tools providing an integrated view of the security situation at any point in time. Records of the following application transactions shall be maintained:
  - (a) Registration;
  - (b) Certification;
  - (c) Publication;
  - (d) Suspension; and
  - (e) Revocation.
- (ii) Records and log files shall be reviewed regularly for the following activities:
  - (a) Misuse;
  - (b) Errors;
  - (c) Security violations;
  - (d) Execution of privileged functions;
  - (e) Change in access control lists;
  - (f) Change in system configuration.

(3) All logs, whether maintained through electronic or manual means, should contain the date and time of the event, and the identity of the subscriber / subordinate / entity which caused the event.

(4) A Certifying Authority should also collect and consolidate, either electronically or manually, security information which may not be generated by his system, such as:

- (i) Physical access logs;

- (ii) System configuration changes and maintenance;
- (iii) Personnel changes;
- (iv) Discrepancy and compromise reports;
- (v) Records of the destruction of media containing key material, activation data, or personal subscriber information.

(5) To facilitate decision-making, all agreements and correspondence relating to services provided by Certifying Authority should be collected and consolidated, either electronically or manually, at a single location.

## **9.2 Frequency of Audit Log Monitoring.-**

The Certifying Authority must ensure that its audit logs are reviewed by its personnel at least once every two weeks and all significant events are detailed in an audit log summary. Such reviews should involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken following these reviews must be documented.

## **9.3 Retention Period for Audit Log.-**

The Certifying Authority must retain its audit logs onsite for at least twelve months and subsequently retain them in the manner described in para 10 of the Information Technology Security Guidelines as given in Schedule-II.

## **9.4 Protection of Audit Log.-**

The electronic audit log system must include mechanisms to protect the log files from unauthorised viewing, modification, and deletion. Manual audit information must be protected from unauthorised viewing, modification and destruction.

## **9.5 Audit Log Backup Procedures.-**

Audit logs and audit summaries must be backed up or copied if in manual form.

## **9.6 Vulnerability Assessments.-**

Events in the audit process are logged, in part, to monitor system vulnerabilities. The Certifying Authority must ensure that a vulnerability assessment is performed, reviewed and revised, if necessary, following an examination of these monitored events.

## **10. Records Archival.-**

(1) Digital Signature Certificates stored and generated by the Certifying Authority must be retained for at least seven year after the date of its expiration. This requirement does not include the backup of private signature keys.

(2) Audit information as detailed in para 9, subscriber agreements, verification, identification and authentication information in respect of subscriber shall be retained for at least seven years.

(3) A second copy of all information retained or backed up must be stored at three locations within the country including the Certifying Authority site and must be protected either by physical security alone, or a combination of physical and cryptographic protection. These secondary sites must provide adequate protection from environmental threats such as temperature, humidity and magnetism. The secondary site should be reachable in few hours.

(4) All information pertaining to Certifying Authority's operation, Subscriber's application, verification, identification, authentication and Subscriber agreement shall be stored within the country. This information shall be taken out of the country only with the permission of Controller and where a properly constitutional warrant or such other legally enforceable document is produced.

(5) The Certifying Authority should verify the integrity of the backups at least once every six months.

(6) Information stored off-site must be periodically verified for data integrity.

## **11. Compromise and Disaster Recovery.**

### **11.1 Computing Resources, Software and/or Data are Corrupted .-**

The Certifying Authority must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing and networking resources, nominated website, repository, software and/or data. Where a repository is not under the control of the Certifying Authority, the Certifying Authority must ensure that any agreement with the repository provides for business continuity procedures.

### **11.2 Secure facility after a natural or other type of disaster.-**

The Certifying Authority must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. Where a repository is not under the control of the Certifying

Authority, the Certifying Authority must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

### **11.3 Incident Management Plan.-**

An incident management plan shall be developed and approved by the management. The plan shall include the following areas:

- (i) Certifying Authority's certification key compromise;
- (ii) Hacking of systems and network;
- (iii) Breach of physical security;
- (iv) Infrastructure availability;
- (v) Fraudulent registration and generation of Digital Signature Certificates; and
- (vi) Digital Signature Certificate suspension and revocation information.

An incident response action plan shall be established to ensure the readiness of the Certifying Authority to respond to incidents. The plan should include the following areas:

- (i) Compromise control;
- (ii) Notification to user community; (if applicable)
- (iii) Revocation of affected Digital Signature Certificates; (if applicable)
- (iv) Responsibilities of personnel handling incidents;
- (v) Investigation of service disruption;
- (vi) Service restoration procedure;
- (vii) Monitoring and audit trail analysis; and
- (viii) Media and public relations.

### **12. Number of Persons Required Per Task.-**

The Certifying Authority must ensure that no single individual may gain access to the Digital Signature Certificate server and the computer server maintaining all information associated with generation, issue and management of Digital Signature Certificate and private keys of the Certifying Authority. Minimum two individuals, preferably using a split-knowledge technique, such as twin passwords, must perform any operation associated with generation, issue and management of Digital Signature Certificate and application of private key of the Certifying Authority.

### **13. Identification and Authentication for Each Role.-**

All Certifying Authority personnel must have their identity and authorisation verified before they are:

- (i) included in the access list for the Certifying Authority's site;
- (ii) included in the access list for physical access to the Certifying Authority's system;
- (iii) given a certificate for the performance of their Certifying Authority role;
- (iv) given an account on the PKI system.

Each of these certificates and accounts (with the exception of Certifying Authority's signing certificates) must:

- (i) be directly attributable to an individual;
- (ii) not be shared;
- (iii) be restricted to actions authorised for that role; and
- (iv) procedural controls.

Certifying Authority's operations must be secured using techniques of authentication and encryption, when accessed across-a shared network.

### **14. Personnel Security Controls.-**

The Certifying Authority must ensure that all personnel performing duties with respect to its operation must:

- (i) be appointed in writing;
- (ii) be bound by contract or statute to the terms and conditions of the position they are to fill;
- (iii) have received comprehensive training with respect to the duties they are to perform;
- (iv) be bound by statute or contract not to disclose sensitive Certifying Authority's security related information or subscriber information;
- (v) not be assigned duties that may cause a conflict of interest with their Certifying Authority's duties; and
- (vi) be aware and trained in the relevant aspects of the Information Technology Security Policy and Security Guidelines framed for carrying out Certifying Authority's operation.

### **15. Training Requirements.-**

A Certifying Authority shall ensure that all personnel performing duties with respect to its operation, must receive comprehensive training in:

- (i) relevant aspects of the Information Technology Security Policy and Security Guidelines framed by the Certifying Authority;
- (ii) all PKI software versions in use on the Certifying Authority's system;
- (iii) all PKI duties they are expected to perform; and
- (iv) disaster recovery and business continuity procedures.

## **16. Retraining Frequency and Requirements.-**

The requirements of para 15 must be kept current to accommodate changes in the Certifying Authority's system. Refresher training must be conducted as and when required, and the Certifying Authority must review these requirements at least once a year.

## **17. Documentation Supplied to Personnel.-**

A Certifying Authority must make available to his personnel the Digital Signature Certificate policies it supports, its Certification Practice Statement, Information Technology Security Policy and any specific statutes, policies or contracts relevant to their position.

## **18. Key Management.**

### **18.1 Generation.-**

(1) The subscriber's key pair shall be generated by the subscriber or on a key generation system in the presence of the subscriber.

(2) The key generation process shall generate statistically random key values that are resistant to known attacks.

### **18.2 Distribution of Keys.-**

Keys shall be transferred from the key generation system to the storage device (if the keys are not stored on the key generation system) using a secure mechanism that ensures confidentiality and integrity.

### **18.3 Storage.-**

(1) Certifying Authority's keys shall be stored in tamper-resistant devices and can only be activated under split-control by parties who are not involved in the set-up and maintenance of the systems and operations of the Certifying Authority. The key of the Certifying Authority may be stored in a tamper-resistant cryptographic module or split into sub-keys stored in tamper-resistant devices under the custody of the key custodians.

(2) The Certifying Authority's key custodians shall ensure that the Certifying Authority's key component or the activation code is always under his sole custody. Change of key custodians shall be approved by the Certifying Authority's management and documented.

### **18.4 Usage.-**

(1) A system and software integrity check shall be performed prior to Certifying Authority's key loading.

(2) Custody of and access to the Certifying Authority's keys shall be under split control. In particular, Certifying Authority's key loading shall be performed under split control.

### **18.5 Certifying Authority's Public Key Delivery to Users.-**

The Certifying Authority's public verification key must be delivered to the prospective Digital Signature Certificate holder in an on-line transaction in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner.

## **19. 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.

## **20. 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.

## **21. Usage Periods for the Public and Private Keys.**

### **21.1 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.

### **21.2 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.

### **21.3 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 unauthorised modification.

### **22. 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.

## **SCHEDULE-IV** **[See rule 23]**

### **FORM FOR APPLICATION FOR ISSUE OF DIGITAL SIGNATURE CERTIFICATE**

For Individual/Hindu Undivided Family Applicant

1. Full Name \* [Name of the Karta in case of Hindu Undivided family]

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. In case of foreign national, visa detail \_\_\_\_\_

10. Credit Card Details

Credit Card Type \_\_\_\_\_  
 Credit Card No. \_\_\_\_\_  
 Issued By \_\_\_\_\_

11. E-mail Address \_\_\_\_\_

12. Web URL address \_\_\_\_\_

13. Passport Details #

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

14. Voter's Identity Card No. # \_\_\_\_\_

15. Income Tax PAN no. # \_\_\_\_\_

16. ISP Details

ISP Name \* \_\_\_\_\_  
 ISP's Website Address, if any \_\_\_\_\_

Your User Name at ISP, if any \_\_\_\_\_

17. Personal Web page URL address, if any \_\_\_\_\_

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. Names, Address etc. of Partners / Members / Directors (for Information about more persons, please add separate sheet (s) in the format given below)\*

Details of Partners/Members/Directors:

No. of Partners/Members/Directors \_\_\_\_\_

Full Name \_\_\_\_\_

Last Name/Surname \_\_\_\_\_

First Name \_\_\_\_\_

Middle Name \_\_\_\_\_

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. \_\_\_\_\_

Nationality \_\_\_\_\_

In case of foreign national, Visa details \_\_\_\_\_

Passport Details #

Passport No. \_\_\_\_\_

Passport issuing authority \_\_\_\_\_

Passport expiry date \_\_\_\_\_  
Voter's Identity Card No. # \_\_\_\_\_  
Income Tax PAN no. # \_\_\_\_\_  
E-mail Address \_\_\_\_\_  
Personal Web page URL, if any \_\_\_\_\_  
For Government Organisations / Agencies  
24. Particulars of Organisation/Agency: \*  
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 \_\_\_\_\_  
25. Bank Details  
Bank Name \* \_\_\_\_\_  
Branch \* \_\_\_\_\_  
Bank Account No. \* \_\_\_\_\_  
Type of Bank Account \* \_\_\_\_\_  
26. Types of Digital Signature Certificate required \*  
27. Any other Detail \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Date \_\_\_\_\_ Signature of the Applicant \_\_\_\_\_

Instructions :

1. Columns marked with \* are mandatory as applicable.
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.
4. Column No. 18 to 23 are to be filled up if applicant is a Company/ Firm/ Body of Individuals / Association of Persons / Local Authority.
5. Column No. 24 is to be filled up if applicant is a Government organisation.
6. Column No. 25 & 16 are to be filled up by all applicants.

## **THE CYBER REGULATIONS APPELLATE TRIBUNAL (PROCEDURE) RULES, 2000**

### **1. Short title and commencement.-**

- (1) These rules may be called the Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000.
- (2) They shall come into force on the date of publication in the Official Gazette.

### **2. Definitions.—**

In these rules, unless the context otherwise requires.—

- (a) "Act" means the Information Technology Act, 2000; (21 of 2000);
- (b) "agent" means a person duly authorised by a party to present an application or reply on its behalf before the Tribunal;
- (c) "application" means an application made to the Tribunal under section 57;
- (d) "legal practitioner" shall have the same meaning as is assigned to it in the Advocates Act, 1961 (25 of 1971);
- (e) "Presiding Officer" means the Presiding Officer of the Tribunal;
- (f) "Registrar" means the Registrar of the Tribunal and includes any officer to whom the powers and functions of the Registrar may be delegated;
- (g) "registry" means the Registry of the Tribunal;
- (h) "section" means a section of the Act;
- (i) "transferred application" means the suit or other proceeding which has been transferred to the Tribunal under sub-section (1) of section 29;
- (j) "Tribunal" means the Cyber Regulations Appellate Tribunal established under section 48.

### **3. Procedure for filing applications.-**

(1) An application to the Tribunal shall be presented in Form-1 annexed to these rules by the applicant in person or by an agent or by a duly authorised legal practitioner, to the Registrar or sent by registered post addressed to the Registrar.

(2) The application under sub-rule (1) shall be presented in six complete sets in a paper-book form along with one empty file size envelope bearing full address of the respondent. Where the number of respondents is more than one, sufficient number of extra paper-books together with required number of empty file size envelopes bearing the full address of each respondent shall be furnished by the applicant.

(3) The applicant may attach to and present with his application a receipt slips as in Form No. 1 which shall be signed by the Registrar or the officer receiving the applications on behalf of-the Registrar in acknowledgement of the receipt of the application.

(4) Notwithstanding anything contained in sub rules (1), (2) and (3), the Tribunal may permit:—

- (a) more than one person to join together and file a single application if it is satisfied, having regard to the cause of action and the nature of relief prayed for, that they have the same interest in the service matter; or
- (b) an Association representing the persons desirous of joining in a single application provided, however, that the application shall disclose the names of all the persons on whose behalf it has been filed.

### **4. Presentation and scrutiny of applications.—**

(1) The Registrar, or the officer authorised by the Registrar shall endorse on every application the date on which it is presented or deemed to have been presented under that rule and shall sign the endorsement.

(2) If, on scrutiny, the application is found to be in order, it shall be duly registered and given a serial number.

(3) If the application, on scrutiny, is found to be defective, and the defect noticed is formal in nature, the Registrar may allow the party to rectify the same in his presence, and if the said defect is not formal in nature, the Registrar may allow the applicant such time to rectify the defect as he may deem fit.

(4) If the applicant fails to rectify the defect within the time allowed under sub rule (3), the Registrar may, by order and for reasons to be recorded in writing, decline to register the application.

(5) An appeal against the order of the Registrar under sub rule (4) shall be made within 15 days of the making of such order to the Tribunal whose decision thereon shall be final.

### **5. Place of filing application.—**

The applicant shall file application with the Registrar.

### **6. Application fee.—**

Every application filed with the Registrar shall be accompanied by a fee of Rs. 2,000/- (rupees two thousand) only which shall be either in the form of a crossed demand draft or a pay order drawn on a Scheduled Bank in favour of the Registrar and payable at New Delhi.

### **7. Contents of application.—**

(1) Every application filed under rule 3 shall set forth concisely under distinct heads, the grounds for such application and such grounds shall be numbered consecutively and typed in double space on one side of the paper.

(2) It shall not be necessary to present a separate application to seek an interim order or direction if the application contains a prayer seeking an interim order or direction pending final disposal of the application.

(3) An application may, subsequent to the filing of application under section 57 of the Act, apply for an interim order or direction. Such an application shall, as far as possible, be in the same form as is prescribed for on application under section 57 and shall be accompanied by a fee of Rs. 5/- (Rupees five only) which shall be payable in court fee stamps affixed on such application.

### **8. Paper book, etc. to accompany the application.-**

(1) Every application shall be accompanied by a paper book containing:—

- (i) a certified copy of the order against which the application has been filed;
- (ii) copies of the documents relied upon by the applicant and referred to in the application; and
- (iii) an index of documents.

(2) The documents referred to in sub rule (1) may be attested by an advocate or by a Gazetted Officer.

(3) Where an Application is filed by an agent, documents authorising him to act as such agent shall also be appended to the application:

Provided that where an application is filed by an advocate it shall be accompanied by a duly executed 'vakalatname'.

### **9. Plural remedies.—**

An application shall be based upon a single cause of action and may seek one or more reliefs provided they are consequential to one another.

### **10. Service of notice of application on the respondents.—**

(1) A copy of the application in the paper-book shall ordinarily be served on each of the respondents by the Registrar in one of the following modes:—

- (i) hand delivery (dasti) through the applicant or through a process server; or
- (ii) through registered post with acknowledgement due.

(2) Notwithstanding anything contained in sub rule (1), the Registrar may, taking into account the number of respondents and their places of residence or work and other circumstances direct that notice of the application shall be served upon the respondents in any other manner including any manner of substituted service, as it appear to the Registrar just and convenient.

(3) Every applicant shall pay a fee for the service or execution of processes, in respect of an application where the number of respondents exceeds five, as under:—

- (1) a sum of Rs. 50 (Rupees fifty) for each respondent in excess of five respondents; or
- (2) where the service is in such manner as the Registrar may direct under sub rule (2), a sum not exceeding the actual charges incurred in effecting the service as may be determined by the Registrar.

(4) The fee for the service or execution of processes under 'sub rule (3) shall be remitted by the applicant either in the form of a crossed Demand Draft drawn on a Scheduled Bank in favour of the Registrar and payable at the station where Registrar's office is situated or remitted through a crossed Indian Postal Order drawn in favour of the Registrar and payable in General Post Office of the station where the Tribunal is located.

(5) Notwithstanding anything contained in sub rules (1), (2), (3) and (4), if the Tribunal is satisfied that it is not reasonably practicable to serve notice of application upon all the respondents, it may for reasons to be recorded in writing, direct that the application shall be heard notwithstanding that some of the respondents have not been served with notice of the application, provided that no application shall be heard unless:—

- (i) notice of the application has been served on the Government, if Government is respondent;
- (ii) notice of the application has been served on the authority which passed the order against which the application has been filed; and

- (iii) the Tribunal is satisfied that the interests of the respondents on whom notice of the application has not been served are adequately and sufficiently represented by the respondents on whom notice of the application has been served.

#### **11. Filing of reply and other documents by the respondent.-**

(1) The respondent shall file six complete sets containing the reply to the application alongwith the documents in a paper-book form with the Registrar within one month of the date of service of the notice of the application on him.

(2) The respondent shall also serve a copy of the reply along with copies of documents as mentioned in sub rule (1) to the applicant or his advocate, if any, and file proof of such service with the Registrar. The Tribunal may, on application by the respondent, allow filing of the reply after the expiry of the period of one month.

#### **12. Date and place of hearing to be notified.—**

The Tribunal shall notify to the parties the date and the place of hearing of the application.

#### **13. Sittings of the Tribunal.—**

The Tribunal shall ordinarily hold its sittings at New Delhi:

Provided that, if at any time, the Presiding Officer of the Tribunal is satisfied that circumstances exist which render it necessary to have sittings of the Tribunal at any place other than New Delhi the Presiding Officer may direct to hold the sittings at any such appropriate place.

#### **14. Decision on applications.—**

(1) Tribunal shall draw up a calendar for the hearing of transferred cases and as far as possible hear and decide the cases according to the calendar.

(2) Every application shall be heard and decided, as far as possible, within six months of the date of its presentation.

(3) For purposes of sub-rule (1) and (2), the Tribunal shall have the power to decline an adjournment and to limit the time for oral arguments.

#### **15. Action on application for applicant's default.—**

(1) Where on the date fixed for hearing of the application or on any other date to which such hearing may be adjourned, the applicant does not appear when the application is called on for hearing, the Tribunal may, in its discretion, either dismiss the application for default or hear and decide it on merit.

(2) Where an application has been dismissed for default and the applicant appears afterwards and satisfies the Tribunal that there was sufficient cause for his non-appearance when the application was called on for hearing, the Tribunal shall make an order setting aside the order dismissing the application and restore the same.

#### **16. Hearing on application *ex-parte*.—**

(1) Where on the date fixed for hearing the application or on any other date to which hearing is adjourned, the applicant appears and the respondent does not appear when the application is called on for hearing, the Tribunal may, in its discretion, adjourn or hear and decide the application *ex-parte*.

(2) Where an application has been heard *ex-parte* against a respondent or respondents, such respondent or respondents may apply to the Tribunal for an order to set it aside and if such respondent or respondents satisfy the Tribunal that the notice was not duly served, or that he or they were prevented by any sufficient cause from appearing when the application was called on for hearing, the Tribunal may make an order setting aside the *ex-parte* hearing as against him or them upon such terms as it thinks fit, and shall appoint a day for proceeding with the application:

Provided that where the *ex-parte* hearing of the application is of such nature that it cannot be set aside as against one respondent only, it may be set aside as against all or any of the other respondents also:

Provided further that Tribunal shall not set aside *ex-parte* hearing of an application merely on the ground that there has been an irregularity in the service of notice, if it is satisfied that the respondent had notice of the date of hearing and had sufficient time to appear and answer the applicant's claim.

#### **17. Adjournment of application.—**

The Tribunal may on such terms as it deems fit and at any stage of the proceedings adjourn the hearing of the application.

#### **18. Order to be signed and dated—**

Every order of the Tribunal shall be in writing and shall be signed and dated by the Presiding Officer.

**19. Publication of orders.—**

Such of the orders of the Tribunal as are deemed fit for publication in any report or the press may be released for such publication on such terms and conditions as the Tribunal may lay down.

**20. Communication of orders to parties.—**

Every order passed on an application shall be communicated to the applicant and to the respondent either in person or by registered post free of cost.

**21. No fee for inspection of records.—**

No fee shall be charged for inspecting the records of a pending application by a party thereto.

**22. Orders and directions in certain cases.—**

The Tribunal may make such orders or give such directions as may be necessary or expedient to give effect or in relation to its orders or to prevent abuse of its process or to secure the ends of justice.

**23. Registration of legal practitioners clerks: —**

(1) A clerk employed by a legal practitioner and permitted as such to have access to the records and to obtain copies of the orders of the Tribunal in which the legal practitioner ordinarily practices shall be known as a "registered clerk".

(2) A legal practitioner desirous of registering his clerk shall make an application to the Registrar in Form 2.

(3) A legal practitioner shall have at a time not more than two registered clerks unless the Registrar by general or special order otherwise permits.

(4) A register of all the registered clerks shall, be maintained in the office of the Registrar and after registration of the clerk, the Registrar shall direct the issue of an identity card to him which shall be non transferable and shall be produced by the holder upon request by an officer or any other employee of the Tribunal.

(5) The identity card mentioned in sub-rule (4) shall be issued under the signatures of the Registrar of the Tribunal.

(6) whenever a legal practitioner ceases to employ a registered clerk, he shall notify the fact at once to the Registrar by means of a letter enclosing therewith the identity card issued to his clerk and on receipt of such letter the name of the said registered clerk shall be struck off from the register.

**24. Working hours of the Tribunal—**

Except on Saturday, Sundays and other holidays, the offices of the Tribunal shall, subject to any order made by the Presiding Officer, remain open daily from 10.00 a.m. to 5.00 p.m. but no work, unless it is of an urgent nature, shall be admitted after 4.30 p.m. on any working day.

**25. Sitting hours of the Tribunal,—**

The sitting hours of the Tribunal shall ordinarily be from 10.30 a.m. to 1-00 p.m. and 2.00 p.m. to 5.00 p.m. subject to any order made by the Chairman.

**26. Powers and functions of the Registrar: —**

(1) The Registrar shall have the custody of the records of the Tribunal and shall exercise such other functions as may be assigned to him under these rules or by the Presiding Officer.

(2) The Registrar may, with the approval of the Presiding Officer, delegate to another officer of the Tribunal any functions required by these rules to be exercised by the Registrar.

(3) In the absence of the Registrar, officer of the Tribunal authorised in writing by the Presiding Officer in his behalf may perform or exercise all or any of the functions and powers of the Registrar.

(4) The Registrar shall keep in his custody the official seal of the Tribunal.

(5) The Registrar shall, subject to any general or special direction by the Presiding Officer, affix the official seal of the Tribunal on any order, notice or other process.

(6) The Registrar shall have the power to authorise in writing the affixing of the seal of the Tribunal on a certified copy of any order of the Tribunal.

**27. Additional powers and duties of Registrar.-**

In addition to the powers conferred elsewhere in these rules, the Registrar shall have the following powers and duties subject to any general or special order of the Presiding Officer namely:—

- (i) to receive all applications and other documents including transferred applications;

- (ii) to decide all questions arising out of the scrutiny of the applications before they are registered;
- (iii) to require any application presented to the Tribunal to be amended in accordance with the Act and the rules;
- (iv) subject to the directions of the Tribunal (to fix dates of hearing of the applications or other proceedings and issue notices thereof);
- (v) to direct any formal amendment of records;
- (vi) to order grant of copies of documents to parties to the proceedings;
- (vii) to dispose of all matters, relating to the service of notices of other processes, applications for the issue of fresh notices or for extending the time therefore;
- (viii) to requisition records from the custody of any court or other authority;
- (ix) to receive applications for the substitution of legal representatives of the deceased parties, during the pendency of the application;
- (x) to receive and dispose of applications for substitution, except where the substitution would involve setting aside an order or abatement; and
- (xi) to receive and dispose of application by parties for return of documents.

**28. Seal and emblem—**

The official seal and emblem of the Tribunal shall be such as the Government may specify.

**FORM-1**  
**(See rule 4)**

**APPLICATION UNDER SECTION 57 OF THE INFORMATION TECHNOLOGY ACT, 2000**

For use in Tribunal's Office

Date of Filing -----

OR

Date of Receipt By post -----

Registration No. -----

Signature of Registrar

In the Cyber Regulations Appellate Tribunal

-----  
-----

BETWEEN

A            B            APPLICANT

AND

C            D            RESPONDENT

Details of application :

**1. Particulars of the applicant:—**

- (i) Name of the applicant
- (ii) Name of Father/Husband
- (iii) Designation and office in which employed
- (iv) Office Address
- (v) Address for service of all notice

**2. Particulars of the respondent :**

- (i) Name and/or designation of the respondent
- (ii) Office address of the respondent
- (iii) Address for service of all notices

**3. Particulars of the Order against which application is made :**

The application is against the following order:

- (i) Order No.
- (ii) Date

- (iii) Passed by
- (iv) Subject in brief

**4. Jurisdiction of the Tribunal:**

The applicant declares that the subject matter of the order against which he wants redressal is within the jurisdiction of the Tribunal.

**5. Limitation.—**

The applicant further declares that the application is within the limitation prescribed in section 57 of the Information Technology Act, 2000.

**6. Fact of the case:—**

The facts of the case are given below:—  
(Give here a concise statement of facts in a chronological order, each paragraph containing as nearly as possible a separate issue, fact or otherwise).

**7. Relief(s) sought:—**

In view of the facts mentioned in para 6 above, the applicant prays for the following relief(s) :—  
[Specify below the relief(s) sought explaining the ground for the relief(s) and the legal provisions (if any) relied upon].

**8. Interim order, if prayed for :**

Pending final decision on the application, the applicant seeks issue of the following interim order :—  
(Give here the nature of the interim order prayed for with reasons).

**9. Details of the remedies exhausted :—**

The applicant declares that he has availed of all the remedies available to him under the relevant service rules, etc.  
(Give here chronologically the details of representations made and the outcome of such representation).

**10. Matter not pending with any other court, etc.—**

The applicant further declares that the matter regarding which this application has been made is not pending before any court of law or any other authority or has not been rejected by any court of law or other authority.

**11. Details of Index :—**

An index in duplicate containing the details of the documents to be relied upon is enclosed.

**12. List of enclosures :—**

**Verification**

I, \_\_\_\_\_ (name of the applicant), S/o, D/o, W/o \_\_\_\_\_ age \_\_\_\_\_  
working as \_\_\_\_\_ resident of \_\_\_\_\_ hereby verify that the contents  
from 1 to 12 are true to my personal knowledge and belief and that I have not suppressed any material facts.

Place :

Date :

Signature of applicant

To  
The Registrar,  
Cyber Regulation Appellate Tribunal  
New Delhi

**RECEIPT SLIP**

Receipt of the application filed in the Cyber Regulation Appellate Tribunal by Shri/Smt. \_\_\_\_\_ working as \_\_\_\_\_ in the Office of \_\_\_\_\_ residing \_\_\_\_\_ acknowledged.

**FORM – 2  
(See Rule 24)**

**APPLICATION FOR THE REGISTRATION OF A CLERK**

1. Name of legal practitioner on whose behalf the clerk is to be registered.
2. Particulars of the clerk to be registered.
  - (i) Full Name (in capitals)
  - (ii) Father's name
  - (iii) Age and date of birth
  - (iv) Place of birth
  - (v) Nationality
  - (vi) Educational qualifications
  - (vii) Particulars of previous employment, if any.

I, \_\_\_\_\_ (clerk above named) do hereby affirm that that the particulars relating to me are true.

3. Whether the legal practitioner has a clerk already registered in his employ and whether the clerk sought to be registered is in lieu of or in addition to the clerk already registered.

4. Whether the clerk sought to be registered is already registered as a clerk of any other legal practitioner and if so, the name of such practitioner.

I, \_\_\_\_\_ (legal practitioner) certify that the particulars given above are true to the best of my information and belief and that I am not aware of any facts which would render undesirable the registration of the said \_\_\_\_\_ (name) as a clerk.

Date:

Signature of legal practitioner

To  
The Registrar of the Tribunal

\_\_\_\_\_  
\_\_\_\_\_

## **INFORMATION TECHNOLOGY (CERTIFYING AUTHORITY) REGULATIONS, 2001**

*In exercise of the powers conferred by clauses (c), (d), (e), and (g) of sub-section (2) of section 89 of the Information Technology Act, 2000 (21 of 2000), the Controller hereby, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, makes the following Regulations, namely: -*

### **1. Short title and Commencement:-**

(1) These Regulations may be called the INFORMATION TECHNOLOGY (CERTIFYING AUTHORITY) REGULATIONS, 2001.

(2) They shall come into force on the date of their publication in the Official Gazette.

### **2. Definitions:-**

In these Regulations, unless the context otherwise requires,-

- (a) "Act" means the Information Technology Act, 2000 (21 of 2000);
- (b) "Certifying Authority" means a person who has been granted a licence to issue a Digital Signature Certificate under section 24 of the Act;
- (c) "Certificate Revocation List" means a periodically (or exigently) issued list, digitally signed by a Certifying Authority, of identified Digital Signature Certificates that have been suspended or revoked prior to their expiration dates;
- (d) "Controller" means the Controller of Certifying Authorities appointed under sub-section (1) section 17 of the Act;
- (e) "Form" means the form appended to these Regulations;
- (f) "Public Key Certificate" means a Digital Signature Certificate issued by Certifying Authority.
- (g) "subscriber" means a person in whose name the Digital Signature Certificate is issued;
- (h) Words and expressions used herein and not defined, but defined in the Act, shall have the meanings respectively assigned to them in the Act.

### **3. Terms and conditions of licence to issue Digital Signature Certificate:-**

Every licence to issue Digital Signature Certificates shall be granted under the Act subject to the following terms and conditions, namely:

#### **(i) General-**

- (a) The licence shall be valid for a period of five years from the date of issue.
- (b) The licence shall not be transferable or heritable;
- (c) The Controller can revoke or suspend the licence in accordance with the provisions of the Act.
- (d) The Certifying Authority shall be bound to comply with all the parameters against which it was audited prior to issue of licence and shall consistently and continuously comply with those parameters during the period for which the licence shall remain valid.
- (e) The Certifying Authority shall subject itself to periodic audits to ensure that all conditions of the licence are consistently complied with by it. As the cryptographic components of the Certifying Authority systems are highly sensitive and critical, the components must be subjected to periodic expert review to ensure their integrity and assurance.
- (f) The Certifying Authority must maintain secure and reliable records and logs for activities that are core to its operations.
- (g) Public Key Certificates and Certificate Revocation Lists must be archived for a minimum period of seven years to enable verification of past transactions.
- (h) The Certifying Authority shall provide Time Stamping Service for its subscribers. Error of the Time Stamping clock shall not be more than 1 in 10.
- (i) The Certifying Authority shall use methods, which are approved by the Controller, to verify the identity of a subscriber before issuing or renewing any Public Key Certificate.
- (j) The Certifying Authority shall publish a notice of suspension or revocation of any certificate in the Certificate Revocation List in its repository immediately after receiving an authorised request of such suspension or revocation.
- (k) The Certifying Authority shall always assure the confidentiality of subscriber information.

- (l) All changes in Certificate Policy and certification practice statement shall be published on the web site of the Certifying Authority and brought to the notice of the Controller well in advance of such publication. However any change shall not contravene any provision of the Act, rule or regulation or made there under.
- (m) The Certifying Authority shall comply with every order or direction issued by the Controller within the stipulated period.

**(ii) Overall Management and Obligations-**

- (a) The Certifying Authority shall manage its functions in accordance with the levels of integrity and security approved by the Controller from time to time.
- (b) The Certifying Authority shall disclose information on the assurance levels of the certificates that it issues and the limitations of its liabilities to each of its subscribers and relying parties.
- (c) The Certifying Authority shall as approved, in respect of security and risk management controls continuously ensure that security policies and safeguards are in place. Such controls include personnel security and incident handling measures to prevent fraud and security breaches.

**(iii) Certificate and Key Management-**

- (a) To ensure the integrity of its digital certificates, the Certifying Authority shall ensure the use of approved security controls in the certificate management processes, i.e. certificate registration, generation, issuance, publication, renewal, suspension, revocation and archival.
- (b) The method of verification of the identity of the applicant of a Public Key Certificates shall be commensurate with the level of assurance accorded to the certificate.
- (c) The Certifying Authority shall ensure the continued accessibility and availability of its Public Key Certificates and Certificate Revocation Lists in its repository to its subscribers and relying parties.
- (d) In the event of a compromise of the private key the Certifying Authority shall follow the established procedures for immediate revocation of the affected subscribers' certificates.
- (e) The Certifying Authority shall make available the information relating to certificates issued and/or revoked by it to the Controller for inclusion in the National Repository.
- (f) The private key of the Certifying Authority shall be adequately secured at each phase of its life cycle, i.e. key generation, distribution, storage, usage, backup, archival and destruction.
- (g) The private key of the Certifying Authority shall be stored in high security module in accordance with FIPS 140-1 level 3 recommendations for Cryptographic Modules Validation List.
- (h) Continued availability of the private key be ensured through approved backup measures in the event of loss or corruption of its private key.
- (i) All submissions of Public Key Certificates and Certificate Revocation Lists to the National Repository of the Controller must ensure that subscribers and relying parties are able to access the National Repository using LDAP ver 3 for X.500 Directories.
- (j) The Certifying Authority shall ensure that the subscriber can verify the Certifying Authority's Public Key Certificate, if he chooses to do so, by having access to the Public Key Certificate of the Controller.

**(iv) Systems and Operations-**

- (a) The Certifying Authority shall prepare detailed manuals for performing all its activities and shall scrupulously adhere to them.
- (b) Approved access and integrity controls such as intrusion detection, virus scanning, prevention of denial-of service attacks and physical security measures shall be followed by the Certifying Authority for all its systems that store and process the subscribers' information and certificates.
- (c) The Certifying Authority shall maintain records of all activities and review them regularly to detect any anomaly in the system.

**(v) Physical, procedural and personnel security-**

- (a) Every Certifying Authority shall get an independent periodic audit done through an approved auditor. Such periodic audits shall focus on the following issues among others :-
  - (i) changes/additions in physical controls such as site location, access, etc;
  - (ii) re-deployment of personnel from an approved role/task to a new one;
  - (iii) appropriate security clearances for outgoing employees such as deletion of keys and all access privileges;
  - (iv) thorough background checks, etc. during employment of new personnel.
- (b) The Certifying Authority shall follow approved procedures to ensure that all the activities referred to in (i) to (iv) in sub-regulation (a) are recorded properly and made available during audits.

**(vi) Financial-**

- (a) Every Certifying Authority shall comply with all the financial parameters during the period of validity of the licence, issued under the Act.
- (b) Any loss to the subscriber, which is attributable to the Certifying Authority, shall be made good by the Certifying Authority.

**(vii) Compliance Audits-**

- (a) The Certifying Authority shall subject itself to Compliance Audits that shall be carried out by one of the empanelled Auditors duly authorised by the Controller for the purpose. Such audits shall be based on the Internet Engineering Task Force document RFC 2527 – Internet X.509 PKI Certificate Policy and Certification Practices Framework.
- (b) If a Digital Signature Certificate issued by the Certifying Authority is found to be fictitious or that proper identification procedures have not been followed by the Certifying Authority while issuing such certificate, the Certifying Authority shall be liable for any losses resulting out of this lapse and shall be liable to pay compensation as decided by the Controller.

**4. The standards followed by the Certifying Authority for carrying out its functions: –**

(1) Every Certifying Authority shall observe the following standards for carrying out different activities associated with its functions.

**(a) PKIX (Public Key Infrastructure)**

Public Key Infrastructure as recommended by Internet Engineering Task Force (IETF) document draft-ietf-pkix-roadmap-05 for “Internet X.509 Public Key Infrastructure” (March 10, 2000);

**(b) Public-key cryptography based on the emerging Institute of Electrical and Electronics Engineers (IEEE) standard P1363 for three families:**

- Discrete Logarithm (DL) systems
- Elliptic Curve Discrete Logarithm (EC) systems
- Integer Factorization (IF) systems;

**(c) Public-key Cryptography Standards (PKCS)**

- PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit)
- PKCS#3 Diffie-Hellman Key Agreement Standard
- PKCS#5 Password Based Encryption Standard
- PKCS#6 Extended-Certificate Syntax 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#11 Cryptographic Token Interface Standard
- PKCS#12 Portable format for storing/transporting a user’s private keys and certificates
- PKCS#13 Elliptic Curve Cryptography Standard
- PKCS#15 Cryptographic Token Information Format Standard;

**(d) Federal Information Processing Standards (FIPS)**

- FIPS 180-1, Secure Hash Standard
- FIPS 186-1, Digital Signature Standard (DSS)
- FIPS 140-1 level 3, Security Requirement for Cryptographic Modules;

**(e) Discrete Logarithm (DL) systems**

- Diffie-Hellman, MQV key agreement
- DSA, Nyberg-Rueppel signatures;

**(f) Elliptic Curve (EC) systems**

- Elliptic curve analogs of DL systems;

**(g) Integer Factorization (IF) systems**

- RSA encryption
- RSA, Rabin-Williams signatures;

**(h) Key agreement schemes**

**(i) Signature schemes**

- DL/EC scheme with message recovery
- PSS, FDH, PKCS #1 encoding methods for IF family
- PSS-R for message recovery in IF family;

**(ii) Encryption schemes**

Abdalla-Bellare-Rogaway DHAES for DL/EC family;

**(i) Form and size of the key pairs**

(1) The minimum key length for Asymmetric cryptosystem (RSA Algorithm) shall be 2048 for the Certifying Authority's key pairs and 1024 for the key pairs used by subscribers.

(2) The Certifying Authority's key pairs shall be changed every three to five years (except during exigencies as in the case of key compromise when the key shall be changed immediately). The Certifying Authority shall take appropriate steps to ensure that key changeover procedures as mentioned in the approved Certificate Practice Statements are adhered to.

(3) The subscriber's key pairs shall be changed every one to two years;

**(j) Directory Services (LDAP ver 3)**

X.500 for publication of Public Key Certificates and Certificate Revocation Lists

X.509 version 3 Certificates as specified in ITU RFC 1422

X.509 version 2 Certificate Revocation Lists;

**(i) Publication of Public Key Certificate.**

The Certifying Authority shall, on acceptance of a Public Key Certificate by a subscriber, publish it on its web site for access by the subscribers and relying parties. The Certifying Authority shall be responsible and shall ensure the transmission of Public Key Certificates and Certificate Revocation Lists to the National Repository of the Controller, for access by subscribers and relying parties. The National Repository shall conform to X.500 Directory Services and provide for access through LDAP Ver 3. The Certifying Authority shall be responsible for ensuring that Public Key Certificates and Certificate Revocation Lists integrate seamlessly with the National Repository on their transmission;

**(k) Public Key Certificate Standard**

All Public Key Certificates issued by the Certifying Authorities shall conform to International Telecommunication Union X.509 version 3 standard. X.509 v3 certificate basic syntax is as follows.

```
tbsCertificate
{
    Version
    Serial Number
    Signature
    Issuer
    Validity
    Subject
    Subject Public Key Information
    Issuer Unique ID [1] IMPLICIT Unique Identifier optional,
        — If present, version shall be v2 or v3
    Subject Unique ID [2] IMPLICIT Unique Identifier optional,
        — If present, version shall be v2 or v3
    Extensions [3] EXPLICIT Extensions optional
        — If present, version shall be v3
}
    Authority Key Identifier
        {
            Key Identifier optional,
            Authority Certificate Issuer optional,
            Authority Certificate Serial Number optional
        }
    Subject Key Identifier
    Key Usage
    {
        Digital Signature
        Non Repudiation
        Key Encipherment
        Data Encipherment
```

```

    Key Agreement
    Key Cert Sign
    cRLSign
    Encipher Only
    Decipher Only
  }
  Private Key Usage Period
  {
    Not Before optional,
    Not After optional
  }
  Certificate Policies
  {
    Policy Information
    {
      Policy Identifier
      Policy Qualifiers optional
    }
    Certificate Policy Id
    {
      Policy Qualifier Info
      {
        Policy Qualifier Id
        Qualifier
        {
          cPSuri
          User Notice
          {
            Notice Reference optional
            {
              Organization
              Notice Numbers
            }
            Display Text optional
            {
              visibleString
              bmpString
              utf8String
            }
          }
        }
      }
    }
  }
  Policy Mappings
  {
    Issuer Domain Policy
    Subject Domain Policy
  }
  Subject Alternative Name
  {
    General Name
    {
      Other Name
      {
        type-id
        value
      }
      Rfc822Name
      DNS Name
      X400 Address
      Directory Name
    }
  }

```

```

edi Party Name
{
    Name Assigner optional,
    Party Name
}
Uniform Resource Identifier
IP Address
Registered ID
}
}
Issuer Alternative Names
Subject Directory Attributes
Basic Constraints
{
    cA
    path Len Constraint optional
}
Name Constraints
{
    Permitted Subtrees optional
    Excluded Subtrees optional
}
Policy Constraints
{
    Require Explicit Policy optional
    Inhibit Policy Mapping optional
}
Extended key usage field
{
    Extended Key Usage Syntax
    Key Purpose Id
    {
        Server Authentication
        Client Authentication
        Code Signing
        Email Protection
        Time Stamping
    }
}
CRL Distribution Points
{
    CRL Distribution Points Syntax
    Distribution Point
    {
        Distribution Point optional
        {
            full Name
            name Relative To CRL Issuer
        }
    }
}
Reasons optional
{
    Unused
    Key Compromise
    CA Compromise
    Affiliation Changed
    Superseded
}

```

```

    Cessation Of Operation
    Certificate Hold
  }
  cRL Issuer optional
}
Authority Information Access
{
    Authority Information Access Syntax
    Access Description
    {
        Access Method
        Access Location
    }
}
}
Signature Algorithm
Signature Value
}

```

**(i) Certificate**

TBSCertificate is certificate “to be signed”. The field contains the names of the subject and issuer, a public key associated with the subject, a validity period, and other associated information. The fields are described in detail.

**(ii) Version**

This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, use X.509 version 3(value is 2). If no extensions are present, but a Unique Identifier is present, use version 2 (value is 1). If only basic fields are present, use version 1 (the value is omitted from the certificate as the default value).

**(iii) Serial number**

The serial number is an integer assigned by the Certifying Authority to each certificate. It shall be unique for each certificate issued by a given Certifying Authority (i.e., the issuer name and serial number identify a unique certificate).

**(iv) Signature**

This field contains the algorithm identifier for the algorithm used by the Certifying Authority to sign the certificate.

**(v) Issuer**

The issuer field identifies the entity who has signed and issued the certificate. The issuer field shall contain a non-empty distinguished name.

**(vi) Validity**

The certificate validity period is the time interval during which the Certifying Authority warrants that it will maintain information about the status of the certificate.

**(vii) Subject**

The subject field identifies the entity associated with the public key stored in the subject public key field. The subject name may be carried in the subject field and/or the Subject Alt Name extension. If the subject is a Certifying Authority (e.g., the basic constraints extension, is present and the value of cA is TRUE,) then the subject field shall be populated with a non-empty distinguished name matching the contents of the issuer field in all certificates issued by the subject Certifying Authority.

**(viii) Subject Public Key Information**

This field is used to carry the public key and identify the algorithm with which the key is used.

**(ix) Unique Identifiers**

These fields may only appear if the version is 2 or 3. The subject and issuer unique identifiers are present in the certificate to handle the possibility of reuse of subject and/or issuer names over time.

**(x) Extensions**

This field may only appear if the version is 3. The extensions defined for X.509 v3 certificates provide methods for associating additional attributes with users or public keys and for managing the certification hierarchy. The X.509 v3 certificate format also allows communities to define private extensions to carry information unique to those communities. If present, this field is a sequence of one or more certificate extensions. The content of certificate extensions in the Internet Public Key Infrastructure is defined as follows, namely:-

## (a) Authority Key Identifier

The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate. This extension is used where an issuer has multiple signing keys (either due to multiple concurrent key pairs or due to changeover). The identification may be based on either the key identifier (the subject key identifier in the issuer's certificate) or on the issuer name and serial number.

## (b) Subject Key Identifier

The subject key identifier extension provides a means of identifying certificates that contain a particular public key.

## (c) Key Usage

The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate. The usage restriction might be employed when a key that could be used for more than one operation is to be restricted. For example, when an RSA key should be used only for signing, the digital Signature and/or non-Repudiation bits would be asserted. Likewise, when an RSA key should be used only for key management, the key Encipherment bit would be asserted.

## (d) Private Key Usage Period

The private key usage period extension allows the certificate issuer to specify a different validity period for the private key than the certificate. This extension is intended for use with digital signature keys. This extension consists of two optional components, not Before and not After. (This profile recommends against the use of this extension. Certifying Authorities conforming to this profile MUST NOT generate certificates with critical private key usage period extensions.)

## (e) Certificate Policies

The certificate policies extension contains a sequence of one or more policy information terms, each of which consists of an object identifier and optional qualifiers. These policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used. Optional qualifiers, which may be present, are not expected to change the definition of the policy.

## (f) Policy Mappings

This extension is used in Certifying Authority certificates. It lists one or more pairs of object identifiers; each pair includes an issuer Domain Policy and a subject Domain Policy. The pairing indicates the issuing Certifying Authority considers its issuer Domain Policy equivalent to the subject Certifying Authority's subject Domain Policy.

## (g) Subject Alternative Name

The subject alternative names extension allows additional identities to be bound to the subject of the certificate. Defined options include an Internet electronic mail address, a Directory Naming Service name, an IP address, and a uniform resource identifier (URI).

## (h) Issuer Alternative Names

This extension is used to associate Internet style identities with the certificate issuer.

## (i) Subject Directory Attributes

The subject directory attributes extension is not recommended as an essential part of this profile, but it may be used in local environments.

## (j) Basic Constraints

The basic constraints extension identifies whether the subject of the certificate is a Certifying Authority and how deep a certification path may exist through that Certifying Authority.

## (k) Name Constraints

The name constraints extension, which MUST be used only in a Certifying Authority certificate, indicates a name space within which all subject names in subsequent certificates in a certification path shall be located. Restrictions may apply to the subject distinguished name or subject alternative names. Restrictions apply only when the specified name form is present. If no name of the type is in the certificate, the certificate is acceptable.

## (l) Policy Constraints

The policy constraints extension can be used in certificates issued to Certifying Authorities. The policy constraints extension constrains path validation in two ways. It can be used to prohibit policy mapping or require that each certificate in a path contain an acceptable policy identifier.

## (m) Extended key usage field

This field indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension field.

- (n) CRL Distribution Points  
The CRL distribution points extension identifies how CRL information is obtained.
- (o) Private Internet Extensions  
This extension may be used to direct applications to identify an on-line validation service supporting the issuing Certifying Authority.
- (p) Authority Information Access  
The authority information access extension indicates how to access Certifying Authority information and services for the issuer of the certificate in which the extension appears. Information and services may include on-line validation services and Certifying Authority policy data.

**(xi) Signature Algorithm**

The Signature Algorithm field contains the identifier for the cryptographic algorithm used by the Certifying Authority to sign this certificate. The algorithm identifier is used to identify a cryptographic algorithm.

**(xii) Signature Value**

The Signature Value field contains a digital signature computed upon the Abstract Syntax Notation (ASN.1) DER encoded tbsCertificate. The ASN.1 DER encoded tbsCertificate is used as the input to the signature function. This signature value is then ASN.1 encoded as a BIT STRING and included in the Certificate's signature field.

**(l) Certificate Revocation List Standard –**

CRL and CRL Extensions Profile - The CRL contents as per International Telecommunications Union standard ver 2 are as follows

**CertificateList**

```

{
  TBSCertList
  {
    Version
    Signature
    Issuer
    This Update
    Next Update
    Revoked Certificates
  }
  User Certificate
  Revocation Date
  Certificate Revocation List Entry Extensions
  {
    Reason Code
    {
      Unspecified
      Key Compromise
      CA Compromise
      Affiliation Changed
      Superseded
      Cessation Of Operation
      Certificate Hold
      Remove From Certificate Revocation List
    }
  }
  Hold Instruction Code
  Invalidation Date
  Certificate Issuer
} optional
Certificate Revocation List Extensions
{
  Authority Key Identifier

```

```

Issuer Alternative Name
Certificate Revocation List Number
Delta Certificate Revocation List Indicator
Issuing Distribution Point
{
    Distribution Point
    Only Contains User Certs
    Only Contains CA Certs
    Only Some Reasons
    Indirect Certificate Revocation List
}
} optional
Signature Algorithm
Signature Value
}

```

**(i) tbsCertList**

The certificate list to be signed, or TBSCertList, is a sequence of required and optional fields. The required fields identify the Certificate Revocation List issuer, the algorithm used to sign the Certificate Revocation List, the date and time the Certificate Revocation List was issued, and the date and time by which the Certifying Authority will issue the next Certificate Revocation List.

Optional fields include lists of revoked certificates and Certificate Revocation List extensions. The Revoked Certificate List is optional to support the case where a Certifying Authority has not revoked any unexpired certificates that it has issued. The profile requires conforming Certifying Authorities to use the Certificate Revocation List extension cRLNumber in all Certificate Revocation Lists issued.

The first field in the sequence is the tbsCertList. This field is itself a sequence containing the name of the issuer, issue date, issue date of the next list, the list of revoked certificates, and optional Certificate Revocation List extensions. Further, each entry on the revoked certificate list is defined by a sequence of user certificate serial number, revocation date, and optional Certificate Revocation List entry extensions. The fields are described in detail, as follows namely:-

**(ii) Version**

This optional field describes the version of the encoded Certificate Revocation List. When extensions are used, as required by this profile, this field **MUST** be present and **MUST** specify version 2 (the integer value is 1).

**(iii) Signature**

This field contains the algorithm identifier for the algorithm used to sign the Certificate Revocation List. This field shall contain the same algorithm identifier as the signature Algorithm field in the sequence Certificate List.

**(iv) Issuer Name**

The issuer name identifies the entity who has signed and issued the Certificate Revocation List. The issuer identity is carried in the issuer name field. Alternative name forms may also appear in the issuer Alternate Name extension. The issuer name field **MUST** contain an X.500 distinguished name (DN). The issuer name field is defined as the X.501 type Name, and **MUST** follow the encoding rules for the issuer name field in the certificate.

**(v) This Update**

This field indicates the issue date of this Certificate Revocation List. This Update may be encoded as UTC Time or Generalised Time. Certifying Authorities conforming to this profile that issue Certificate Revocation Lists **MUST** encode This Update as UTCTime for dates through the year 2049. Certifying Authorities conforming to this profile that issue Certificate Revocation Lists **MUST** encode This Update as Generalised Time for dates in the year 2050 or later.

**(vi) Next Update**

This field indicates the date by which the next Certificate Revocation List will be issued. The next Certificate Revocation List could be issued before the indicated date, but it will not be issued any later than the indicated date. Certifying Authorities should issue Certificate Revocation Lists with a Next Update time equal to or later than all previous Certificate Revocation Lists. Next Update may be encoded as UTCTime or GeneralisedTime.

**(vii) Revoked Certificates**

Revoked certificates are listed. The revoked certificates are named by their serial numbers. Certificates revoked by the Certifying Authority are uniquely identified by the certificate serial number. The date on which the revocation occurred is specified. Additional information may be supplied in Certificate Revocation List entry extensions;

**(viii) CRL Entry Extensions**

The Certificate Revocation List entry extensions already defined by American National Standards Institute X9 and International Standards Organisation /IEC /International telecommunication Union for X.509 v2 Certificate Revocation Lists provide methods for associating additional attributes with Certificate Revocation List entries [X.509] [X9.55]. The X.509 v2 Certificate Revocation List format also allows communities to define private Certificate Revocation List entry extensions to carry information unique to those communities. All Certificate Revocation List entry extensions used in this specification are non-critical.

(a) Reason Code

The reason Code is a non-critical Certificate Revocation List entry extension that identifies the reason for the certificate revocation. Certifying Authorities are strongly encouraged to include meaningful reason codes in Certificate Revocation List entries; however, the reason code Certificate Revocation List entry extension should be absent instead of using the unspecified (0) Reason Code value.

(b) Hold Instruction Code

The hold instruction code is a non-critical Certificate Revocation List entry extension that provides a registered instruction identifier, which indicates the action to be taken after encountering a certificate that has been placed on hold.

(c) Invalidity Date

The invalidity date is a non-critical Certificate Revocation List entry extension that provides the date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid. This date may be earlier than the revocation date in the Certificate Revocation List entry, which is the date at which the Certifying Authority processed the revocation.

(d) Certificate Issuer

This Certificate Revocation List entry extension identifies the certificate issuer associated with an entry in an indirect Certificate Revocation List, i.e. a Certificate Revocation List that has the indirect Certificate Revocation List indicator set in its issuing distribution point extension. If this extension is not present on the first entry in an indirect Certificate Revocation List, the certificate issuer defaults to the Certificate Revocation List issuer. On subsequent entries in an indirect Certificate Revocation List, if this extension is not present, the certificate issuer for the entry is the same as that for the preceding entry.

**(ix) Issuing Distribution Point**

The issuing distribution point is a critical Certificate Revocation List extension that identifies the Certificate Revocation List distribution point for a particular Certificate Revocation List, and it indicates whether the Certificate Revocation List covers revocation for end entity certificates only, Certifying Authority certificates only, or a limited set of reason codes. Although the extension is critical, conforming implementations are not required to support this extension.

**(x) Signature Algorithm**

The signature Algorithm field contains the algorithm identifier for the algorithm used by the Certifying Authority to sign the Certificate List. This field MUST contain the same algorithm identifier as the signature field in the sequence tbsCertList.

**(xi) Signature Value**

(1) The signature Value field contains a digital signature computed upon the ASN.1 DER encoded to be signed CertList. The ASN.1 DER encoded tbsCertList is used as the input to the signature function. This signature value is then ASN.1 encoded as a BIT STRING and included in the Certificate Revocation List's signature Value field.

(2) The list of standards specified in sub-regulation (1) shall be updated at least once a year to include new standards that may emerge from the international bodies. In addition, if any Certifying Authority or a group of Certifying Authorities brings a set of standards to the Controller for a specific user community, the Controller shall examine the same and respond to them within ninety days.

**5. Every Certifying Authority shall disclose :-**

- (1) (a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;

- (b) any Certification Practice Statement relevant thereto;
- (c) notice of the revocation or suspension of its Certifying Authority Certificate, if any; and
- (d) any other fact that materially or adversely affect either the reliability of a Digital Signature Certificate, which that Authority has issued by it or the Authority's ability to perform its services

(2) The above disclosure shall be made available to the Controller through filling up of online forms on the Web site of the Controller on the date and time the information is made public. The Certifying Authority shall digitally sign the information.

**6. Communication of compromise of Private Key.-**

(1) Where the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, the subscriber shall communicate the same without any delay to the Certifying Authority.

(2) An application for revocation of the key pair shall made in Form online on the web site of the concerned Certifying Authority to enable revocation and publication in the Certificate Revocation List. The Subscriber shall encrypt this transaction by using the public key of the Certifying Authority. The transaction shall be further authenticated with the private key of the subscriber even though it may have already been compromised.

**FORM**  
**[See Regulation 6]**  
**COMMUNICATION OF COMPROMISE OF PRIVATE KEY**

- 1. Name of Holder : \_\_\_\_\_
- 2. Public Key of Holder : (Attach PKC)
- 3. Category of Certificate : Individual/Organisation/Web Server ...../Other (please specify)
- 4. e-mail address : \_\_\_\_\_
- 5. Distinguished Name : \_\_\_\_\_
- 6. Serial No. of Certificate : \_\_\_\_\_
- 7. Certificate Fingerprint : \_\_\_\_\_
- 8. Date & Time of communication : \_\_\_\_\_

(Digital Signature of Holder)

## **CYBER REGULATIONS APPELLATE TRIBUNAL (PROCEDURE FOR INVESTIGATION OF MISBEHAVIOUR OR INCAPACITY OF PRESIDING OFFICER) RULES, 2003**

*In exercise of the powers conferred by clause (s) of sub section (2) of section 87, read with subsection (3) of section 54 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely-*

### **1. Short title and commencement.-**

(1) These rules may be called the CYBER REGULATIONS APPELLATE TRIBUNAL (PROCEDURE FOR INVESTIGATION OF MISBEHAVIOUR OR INCAPACITY OF PRESIDING OFFICER) RULES, 2003.

(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 requires, -

- (a) "Act" means the Information Technology Act, 2000 (21 of 2000);
- (b) "Committee" means a Committee constituted under sub-rule (2) of rule 3;
- (c) "Presiding Officer" means Presiding Officer of the Tribunal appointed under section 49 of the Act;
- (d) "Tribunal" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48 of the Act;
- (e) words and expressions used herein and not defined but defined in the Act shall have the meaning respectively assigned to them in the Act.

### **3. Committee for investigation of complaints.-**

(1) If a written complaint, alleging any definite charges of misbehaviour or incapacity to perform the functions of the offices in respect of a Presiding Officer, is received by the Central Government, it shall make a preliminary scrutiny of such complaint.

(2) If on preliminary scrutiny, the Central Government considers it necessary to investigate into the allegation, it shall place the complaint together with supporting material as may be available, before a Committee consisting of the following officers to investigate the charges of allegations made in the complaint;-

- (i) Secretary (Co-ordination and Public Grievances) Cabinet Secretariat - Chairman;
- (ii) Secretary, Department of Information Technology - Member;
- (iii) Secretary, Department of Legal Affairs, Ministry of Law and Justice -- Member.

(3) The Committee shall devise its own procedure and method of investigation, which may include recording of evidence of the complainant and collection of material relevant to the inquiry which may be conducted by a Judge of the Supreme Court under these rules.

(4) The Committee shall submit its findings to the President as early as possible within a period that may be specified by the President in this behalf.

### **4. Judge to conduct inquiry—**

(1) If the President is of the opinion that there are reasonable grounds for making an inquiry into the truth of any imputation of misbehaviour or incapacity of a Presiding Officer, he shall make a reference to the Chief Justice of India requesting him to nominate a Judge of the Supreme Court to conduct the inquiry.

(2) The President shall, by order, appoint the Judge of the Supreme Court nominated by the Chief Justice of India (hereinafter referred to as Judge) for the purpose of conducting the inquiry.

(3) Notice of appointment of a Judge under sub-rule (2) shall be given to the Presiding Officer,

(4) The President shall forward to the Judge a copy of-

- (a) the articles of charges against the Presiding Officer concerned and the statement of imputations;
- (b) the statement of witnesses, if any; and
- (c) material documents relevant to the inquiry.

(5) The Judge appointed under sub-rule (2) shall complete the inquiry within such time or further time as may be specified by the President.

(6) The Presiding Officer concerned shall be given a reasonable opportunity of presenting a written statement of defence within such time as may be specified in this behalf by the Judge.

(7) Where it is alleged that the Presiding Officer concerned is unable to discharge the duties of his office efficiently due to any physical or mental incapacity and the allegation is denied, the Judge may arrange for the medical

examination of the Presiding officer by such Medical Board as may be appointed for the purpose by the President and the Presiding Officer concerned shall submit himself to such medical examination within the time specified in this behalf by the Judge.

(8) The Medical Board shall undertake such medical examination of the Presiding Officer as may be considered necessary to and submit a report to the Judge stating therein whether the incapacity is such as to render the Presiding Officer unfit to continue in office.

(9) If the Presiding Officer refuses to undergo such medical examination as considered necessary by the Medical Board, the Board shall submit a report to the Judge stating therein the examination which the Presiding Officer has refused to undergo, and the Judge may, on receipt of such report, presume that the Presiding Officer suffers from such physical or mental incapacity as is alleged in the Presiding Officer.

(10) The Judge may, after considering the written statement of the Presiding Officer and the Medical Report, if any, amend the charges referred to in clause (a) of sub-rule (4) and in such case, the Presiding Officer shall be given a reasonable opportunity of presenting a fresh written statement of defence.

(11) The Central Government shall appoint an officer of that Government or an advocate to present the case against the Presiding Officer.

(12) Where the Central Government has appointed an advocate to present its case before the Judge, the Presiding Officer concerned shall also be allowed to present his case by an advocate chosen by him.

#### **5. Application of the Departmental Inquiries (Enforcement of Witness and Production of Documents) Act, 1972 to inquiries under these rules.-**

The provisions of the Departmental Inquiries (Enforcement of Witness and Production of Documents) Act, 1972 (18 of 1972), shall apply to the inquiries made under these rules as they apply to departmental inquiries.

#### **6. Powers of Judge.-**

The Judge shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and shall have power to regulate his own procedure including the fixing of places and times of his inquiry.

#### **7. Suspension of Presiding Officer.-**

Notwithstanding anything contained in rule 4 and without any prejudice to any action being taken in accordance with the said rule, the President, keeping in view the gravity of charges may suspend the Presiding Officer of the Tribunal against whom a complaint is under investigation or inquiry.

#### **8. Subsistence allowance.-**

The payment of subsistence allowance to a Presiding Officer under suspension shall be regulated in accordance with the rules and orders for the time being applicable to a Secretary to the Government of India belonging to the Indian Administrative Service.

#### **9. Inquiry Report.-**

After the conclusion of the investigation, the Judge shall submit his report to the President stating therein his findings and the reasons therefore on each of the articles of charges separately with such observations on the whole case as he thinks fit.

## **INFORMATION TECHNOLOGY (OTHER POWERS OF CIVIL COURT VESTED IN CYBER APPELLATE TRIBUNAL) RULES 2003**

*In exercise of the powers conferred by clause (v) of subsection (2) of section 87, read with clause (g) of sub-section (2) of section 58 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely: -*

### **1. Short title and commencement.-**

(1) These rules may be called THE INFORMATION TECHNOLOGY (OTHER POWERS OF CIVIL COURT VESTED IN CYBER APPELLATE TRIBUNAL) RULES 2003.

(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 requires,-

- (a) "Act" means the Information Technology Act, 2000 (21 Of 2000);
- (b) "Cyber Appellate Tribunal" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48 of the Act;
- (c) words and expressions used herein and not defined but defined in the Act shall have the meaning respectively assigned to them in the Act.

### **3. Powers of Cyber Appellate Tribunal.-**

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

- (a) setting aside any order of dismissal of any application for default or any order passed by it, *ex parte* ;
- (b) requisitioning of any public record, document or electronic record from any court or office.

## **INFORMATION TECHNOLOGY (OTHER STANDARDS) RULES, 2003**

*In exercise of the powers conferred by clause (g) of subsection (2) of section 87, read with sub-section (2) of section 20 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely: -*

### **1. Short title and commencement.-**

(1) These rules may be called THE INFORMATION TECHNOLOGY (OTHER STANDARDS) RULES, 2003.

(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 requires,-

- (a) "Act" means the Information Technology Act, 2000 (21 Of 2000);
- (b) "Controller" means the Controller of Certifying Authorities appointed under sub-section (1) of section 17 of the Act;
- (c) "digital signature" means authentication of any electronic record by subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the Act;
- (c) words and expressions used herein and not defined but defined in the Act shall have the meaning respectively assigned to them in the Act.

### **3. Standards to be observed by the Controller –**

The Controller shall, observe the standards laid down in the Information Technology Security Guidelines and security Guidelines for Certifying Authorities referred to in the Information Technology (certifying Authorities ) Rules, 2000, to ensure that the secretary and security of the digital signatures are assured.

## **THE INFORMATION TECHNOLOGY (QUALIFICATION AND EXPERIENCE OF ADJUDICATING OFFICERS AND MANNER OF HOLDING ENQUIRY) RULES, 2003**

*In exercise of the powers conferred by clause (p) and (q) of sub-section (2) of section 87, of section Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely: -*

### **1. Short title and commencement: -**

(1) These rules may be called THE INFORMATION TECHNOLOGY (QUALIFICATION AND EXPERIENCE OF ADJUDICATING OFFICERS AND MANNER OF HOLDING ENQUIRY) RULES, 2003.

(2) These shall come into force on the date of their publication in the Official Gazette.

### **2. Definitions: -**

In these rules, unless the context otherwise requires –

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

(b) "Adjudicating Officer" means an adjudicating officer appointed under subsection (1) of section 46, of the Act.

(c) "Proforma" means a proforma appended to these rules.

(d) Words and expressions used herein and not defined but defined in the Act shall have the meaning respectively assigned to them in the Act.

### **3. Eligibility for Adjudicating Officer: -**

Whereas the purpose and intent of Section 46(3) of Information Technology Act is that the Adjudicating Officer should be a person so qualified and experienced to take decisions with a view in relation to Information Technology aspects as well as in a position to determine the complaints keeping in view the legal or judicial mannerism on the principle of compensation of damages of Information Technology Act.

A person shall not be qualified for appointment as adjudicating Officer unless the person –

(a) Possesses a University graduate Bachelor degree or equivalent, recognised by Central Government / State Government for the purpose of recruitment to Grade I Service in a Government Department through Union / State Public Service Commission;

(b) Possesses Information Technology experience in the areas of relevance to public interface with Central / State Government functioning and experience obtained through the in-service training imparting competence to operate computer system to send and receive e-mails or other information through the computer network, exposure and awareness about the method of carrying information, data, sound, images or other electronic records through the medium of network including Internet.

(c) Possesses legal or judicial experience to discharge responsibilities connected with the role of Central / State Government in respect of making decisions or orders in relation to administration of laws as a District Magistrate, or Additional District Magistrate or Sub-Divisional Magistrate or an Executive Magistrate or in other administrative or quasi-judicial capacity for a cumulative period of 5 years;

(d) Is working and holding a post in Grade I in Government Department either in State Government/Union Territories to perform functional duty & discharge job responsibility in the field of Information Technology;

(e) Is an in-service officer not below the rank of Director to the Government of India or an equivalent officer of State Government

### **4. Scope and Manner of holding inquiry: -**

(a) The Adjudicating Officers shall exercise jurisdiction in respect of the contraventions in relation to Chapter IX of IT Act 2000 and the matter or matters or places or area or areas in a State or Union Territory of the posting of the person.

(b) The complaint shall be made to the Adjudicating Officer of the State or Union Territory on the basis of location of Computer System, Computer Network as defined in sub-Section 2 of Section 75 of IT Act on a plain paper on the

Proforma attached to these Rules together with the fee payable calculated on the basis of damages claimed by way of compensation.

(c) The Adjudicating Officer, shall issue a notice together with all the documents to all the necessary parties to the proceedings, fixing a date and time for further proceedings. The notice shall contain such particulars as far as may be as to the time and place of the alleged contravention, and the person (if any) against whom, or the thing (if any) in respect of which, it was committed.

- (d) On the date so fixed, the Adjudicating Officer shall explain to such person or persons to whom notice is issued about the contravention alleged to have been committed in relation to any of the provisions of the Act or of any rule, regulation, direction or order made thereunder.
- (e) If the person in respect of whom notice is issued pleads guilty, the Adjudicating Officer shall record the plea, and may impose penalty or award such compensation as he thinks fit in accordance with the provisions of the Act, rules, regulations, order or directions made there under.
- (f) Alternatively on the date fixed the person or persons against whom a matter is filed may show cause why an enquiry should not be held in the alleged contravention or that why the report alleging the contravention should be dismissed.
- (g) The Adjudicating Officer on the basis of the report of the matter, investigation report (if any), other documents and on the basis of submissions shall form an opinion that there is sufficient cause for holding an enquiry or that the report into the matter should be dismissed and on that basis shall either by order dismiss the report of the matter, or shall determine to hear the matter.
- (h) If any person or persons fails, neglects or refuses to appear, or present himself as required by sub-rule (d), before the Adjudicating Officer, the Adjudicating Officer shall proceed with the inquiry in the absence of such person or persons after recording the reasons for doing so.
- (i) At any time or on receipt of a report of contravention from an aggrieved person, or by a Government agency or suo-moto, the Adjudicating Officer, may get the matter or the report investigated from an officer in the Office of Controller or CERT-IND or from the concerned Deputy Superintendent of Police, to ascertain more facts and whether *prima facie* there is a case for adjudicating on the matter or not.
- (j) The Adjudicating Officer, shall fix a date and time for production of documents or evidence and for this purpose may also rely on electronic records or communications and as far as may be, shall use or make available the infrastructure for promoting on-line settlement of enquiry or disputes or for taking evidence including the services of an adjudicating officer and infrastructure in another State.
- (k) As far as possible, every application shall be heard and decided in four months and the whole matter in six months.
- (l) Adjudicating Officer, when convinced that the scope of the case extends to the Offence(s) (under Chapter XI of IT Act) instead of Contravention, needing appropriate punishment instead of mere financial penalty, should transfer the case to the Magistrate having jurisdiction to try the case, through Presiding Officer.

#### **5. Order of the Adjudicating Officer: -**

- (a) If, upon consideration of the evidence produced before the Adjudicating Officer and other records and submissions, the Adjudicating Officer is satisfied that the person has become liable to pay damages by way of compensation or to pay penalty under any of the provisions of the Act or rules, regulations, directions or orders, the Adjudicating Officer may, by order in writing, order payment of damages by way of compensation or impose such penalty, as deemed fit.
- (b) While adjudging the quantum of compensation or penalty, the Adjudicating Officer shall have due regard to the following factors, namely:
  - (i) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
  - (ii) the amount of loss caused to any person as a result of the default;
  - (iii) the repetitive nature of the default.

#### **6. Copy of the Order: -**

Adjudicating Officers shall deliver a certified copy of the order to the Complainant & Respondent.

#### **7. Service of notices and orders: -**

A notice or an order issued under these rules shall be served on the person in any of the following manners, that is to say: -

- (a) by delivering or tendering it to that person or the person's authorised agent in an electronic form provided that there is sufficient evidence of actual delivery of the electronic record to the concerned person; or
- (b) by sending it to the person by registered post with acknowledgement due to the address of his place of residence or the last known place of residence or business place;
- (c) if it cannot be served under clause (a) or (b) above then by affixing it, in the presence of two witnesses, on the outer door or some other conspicuous part of the premises in which that person resides or is known to have last resided, or carried on business or personally works or last worked for gain.

#### **8. Fee: -**

Every complaint of a matter to the Adjudicating Officer shall be accompanied by fee, payable by a bank draft drawn in favour of "Adjudicating Officer Information Technology Act" at the place of functioning of Adjudicating Officer in the States or Union Territories, calculated on the basis of the damages claimed by way of compensation from the contraveners on the rates provided below.

#### TABLE OF FEE

I] Damages by way of compensation	Fee
(a) Upto Rs.10,000	10% <i>ad valorem</i> rounded of to nearest next hundred
(b) From 10,001 to Rs. 50,000/-	Rs. 1000 plus 5% of the amount exceeding Rs.10,000 rounded of to nearest next hundred
(c) From Rs.50,001 to Rs. 1,00,000/-	Rs.3000/- plus 4%of the amount exceeding Rs. 50,000/- rounded of to nearest next hundred
(d) More than Rs. 1,00,000/-	Rs.5000/- plus 2% of the Amount exceeding Rs. 1,00,000 rounded of to nearest next hundred.
II] Fee for every application	Rs. 50/-

#### 9. Duplicity Avoided: -

When an adjudication into a matter of contravention is pending before an Adjudicating Officer, same matter shall not be pursued before any court or Tribunal or Authority in any proceeding whatsoever and if there is already filed a report in relation to the same matter, the proceedings before such other court, Tribunal or Authority shall be deemed to be withdrawn.

#### 10. Frivolous complaints: -

If a person files a frivolous report of the matter, the adjudicating officer in his discretion may order the complainant, to make good the cost of the persons against whom the complaint was filed and to pay a damage of not exceeding Rupees Twenty Five Thousand and the adjudicating officer may also order payment of a fine up to an amount not exceeding Rupees Ten Thousand only.

#### 11. Compounding of Contraventions: -

(a) A person, against whom a report of contravention of the Act, Rules or Regulations, directions or orders or conditions has been filed before an Adjudicating Officer, may make an application for compounding the contravention during the adjudicating proceedings to the concerned adjudicating officer:

Provided that an application for compounding may be filed even before the contravention is reported, in which case the contravener himself shall state the contravention undertaken or committed and the likely loss to various parties and the amount of compensatory damages tendered by the contravener.

(b)The applicant desirous of compounding the contravention shall deposit the sum determined by the officer compounding the contravention into the office of Adjudicating Officer:

Provided that sum determined as compounding fee shall not exceed the maximum amount of penalty, which may be imposed under this Act for the contraventions so compounded.

#### 12. Certifying Authorities and other Governmental Agencies to Assist

All the licensed or recognised Certifying Authorities, the Controller and other officers agencies established under the Act and other government agencies like CERT-IND shall promptly assist the Adjudicating Officers in any proceedings filed or pending before the Adjudicating Officers.

**APPENDIX**  
**PROFORMA FOR COMPLAINT TO ADJUDICATING OFFICER UNDER**  
**INFORMATION TECHNOLOGY ACT, 2000**

- I 1. Name of the Complainant  
2. E-mail address  
3. Telephone No.  
4. Address for correspondence  
5. Digital Signature Certificate, if any
- II 1. Name of the Respondent  
2. E-mail address  
3. Telephone No.  
4. Address for correspondence  
5. Digital Signature Certificate, if any
- III Damages claimed  
Fee deposited  
Demand Draft No. \_\_\_\_\_ dated \_\_\_\_\_ Branch \_\_\_\_\_
- IV Complaint under Section/Rule/Direction/Order etc.
- V Time of Contravention
- VI Place of Contravention
- VII Cause of action
- VIII Brief facts of the case

(Signature of the Complainant)

**THE CYBER REGULATIONS APPELLATE TRIBUNAL (SALARY, ALLOWANCE AND  
OTHER TERMS AND CONDITIONS OF SERVICE OF PRESIDING OFFICER) RULES, 2003**

*In exercise of the powers conferred by clauses (r) of sub-section (2) of Section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules regulating the terms and conditions of the service of the Presiding Officer, namely: -*

**1. Short title and commencement:-**

(1) These rules may be called THE CYBER REGULATIONS APPELLATE TRIBUNAL (SALARY, ALLOWANCES AND OTHER TERMS AND CONDITIONS OF SERVICE OF PRESIDING OFFICER) RULES, 2003.

(2) They shall come into force on the date of their publications in the Official Gazette

**2. Definitions:-**

In these rules, unless the context otherwise requires-

- (a) "Cyber Appellate Tribunal" means Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48;
- (b) "Presiding Officer" means a person appointed as Presiding Officer of a Cyber Appellate Tribunal under section 49 of the Act;
- (c) Words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act;

**3. Salary and Allowances: -**

The Presiding Officer shall be paid such salary and allowances, as admissible to a Secretary to the Government of India, including all the benefits that a Secretary is entitled to. The Presiding Officer shall be deemed to be public servant as per the Section 82 of Information Technology Act 2000 (21 of 2000).

Provided that in the case of appointment of a person as Presiding Officer, who has retired as a Judge of a High Court or who has retired from service under the Central Government or a State Government and who is in receipt of, or has received, or has become entitled to receive any retirement benefits by way of pension, gratuity, employer's contribution to the Provident Fund or other forms of retirement benefits, the pay of such Presiding Officer shall be reduced by the gross amount of pension or employer's contribution to the Provident Fund or any other form of retirement benefit, if any, drawn or to be drawn by him.

Provided further that in case a retired Judge of a High Court is appointed as Presiding Officer, the terms and conditions of service of such Presiding Officer shall be in accordance with the instructions issued by the Ministry of Finance in respect of appointment of Judges to various Tribunals and in consultation with that Ministry.

**4. Leave: -**

A person, on appointment as a Presiding Officer in a Cyber Appellate Tribunal shall be entitled to leave as applicable to the Secretary to the Government of India in respect of Earned Leave, Half Pay Leave, Extra Ordinary Leave, Commutation of Leave, Casual Leave etc.

**5. Leave Sanctioning Authority: -**

The Secretary, Department of Information Technology, Government of India, shall be the authority competent to sanction leave to the Presiding Officer.

**6. Pension or Provident Fund: -**

(i) In case a serving Judge of a High Court or a member of the Indian Legal Service is holding the post of Presiding Officer, the service rendered in the Cyber Appellate Tribunal shall count for pension, to be drawn in accordance with the rules of the service to which he belongs, and he shall also be governed by the provisions of the Provident Fund (Central Services) Rules, 1960.

(ii) In all other cases, the Presiding Officer shall be governed by the provision of the Provident Fund (India) Rules, 1962.

**7. Travelling Allowances: -**

The Presiding Officer while on tour (including the journey undertaken on the expiry of his term with the Cyber Appellate Tribunal to proceed to his home town) shall be entitled to the travelling allowances, daily allowances, transportation of personal effects and other similar matters at the same scales and at the same rates as are applicable to Secretary to the Government of India.

**8. Leave Travel Concession: -**

The Presiding Officer shall be entitled to avail leave travel concession as admissible to the Secretary to the Government of India.

**9. Facility of Conveyance: -**

The Presiding Officer shall be entitled to hire a Taxi on whole time basis in accordance with the rules or orders for the time being in force for hire of taxi by a Secretary to the Government of India.

**10. Accommodation: -**

The presiding Officer shall be entitled to the house rent allowance at the same rate as are, for the time being, admissible to Group "A" officer of the Central Government drawing equivalent pay.

**11. Facilities for medical treatment: -**

The Presiding Officer shall be entitled to medical treatment and hospital facilities, as provided in the Central Government Health Scheme Rules, 1954 and in places where the Central Government Health Scheme is not in operation, the said Presiding Officer shall be entitled to the facilities as provided in the Central Services (Medical Attendance) Rules, 1944.

**12. Residuary Provision: -**

Matters relating to the conditions of service of the Presiding Officer with respect to which no express provision has been made in these rules shall be as per the rules applicable to Group 'A' officers of Central Government.

## **INFORMATION TECHNOLOGY (USE OF ELECTRONIC RECORDS AND DIGITAL SIGNATURES) RULES, 2004**

*In exercise of the powers conferred by clauses (b) and (c) of sub-section (2) of Section 87, read with sub-sections (1) and (2) of Section 6 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:-*

### **1. Short title and commencement--**

(1) These rules may be called THE INFORMATION TECHNOLOGY (USE OF ELECTRONIC RECORDS AND DIGITAL SIGNATURES) RULES, 2004.

(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 requires:--

- (a) "Act" means the Information Technology Act, 2000 (21 of 2000);
- (b) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;
- (c) words and expressions used herein and not defined but defined in the Act shall have the meaning respectively assigned to them in the Act.

### **3. Filing of form, application or any other document.-**

Any form, application or any other document referred to in clause (a) of subsection (1) of Section 6 of the Act may be filed with any office, authority, body or agency owned or controlled by the appropriate Government using the software specified by it and such office, authority, body or agency shall, while generating such software, take into account the following features of the electronic record, namely:-

- (a) lifetime;
- (b) preservability;
- (c) accessibility;
- (d) readability;
- (e) comprehensibility in respect of linked information;
- (f) evidentiary value in terms of authenticity and integrity;
- (g) controlled destructibility; and
- (h) augmentability.

### **4. Issue or grant of any licence, permit, sanction or approval.-**

Any licence, permit, sanction or approval whatever name called referred to in clause (b) of sub-section (1) of Section 6 of the Act may be issued or granted by using the software specified under rule 3.

### **5. Payment and receipt of fee or charges.-**

The payment of receipt of any fee or charges for filing, creation or issue of any electronic record under clause (a) of sub-section (2) of Section 6 of the Act may be made in a cheque in the electronic form.

**Explanation.-** For the purposes of this rule, "a cheque in the electronic form" has the meaning assigned to it in clause (a) of *Explanation 1* to Section 6 of the Negotiable Instrument Act, 1881 (26 of 1881).

## **THE INFORMATION TECHNOLOGY (SECURITY PROCEDURE) RULES, 2004**

*In exercise of the powers conferred by clause (e) of sub-section (2) of section 87, read with section 16 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:-*

### **1. Short title and commencement.-**

- (1) These rules may be called THE INFORMATION TECHNOLOGY (SECURITY PROCEDURE) RULES, 2004
- (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 requires,-

- (a) "Act" means the information Technology Act, 2000 (21 of 2000);
- (b) "Digital signature" means authentication of any electronic records by a subscriber by means of an electronic method of procedure in accordance with the provision of section 3 of the Act;
- (c) "Hardware token" means a token which can be connected to any computer system using Universal Serial Bus (USB) port;
- (d) "Smart card" means a device containing one or more integrated circuit chips, which perform the functions of a computer's centre processor, memory and input or output interface;
- (e) Words and expressions used in these rules and not defined but defined in the Act shall have the meaning respectively assigned to them in the Act.

### **3. Secure electronic record.-**

An electronic record shall be deemed to be a secure electronic record for the purposes of the Act if it has been authenticated by means of a secure digital signature.

### **4. Secure digital signature.-**

A digital signature shall be deemed to be a secure digital signature for the purposes of the Act if the following procedure has been applied to it, namely:-

- (a) That the smart card or hardware token, as the case may be, with cryptographic module, in it, is used to create the key pair;
- (b) That the private key used to create the digital signature always remains in the smart card or hardware token as the case may be;
- (c) That the hash of the content to be signed is taken from the host system to the smart card or hardware token and the private key is used to create the digital signature and the signed hash is returned to the host system;
- (d) That the information contained in the smart card or hardware token, as the case may be, is solely under the control of the person who is purported to have created the digital signature;
- (e) That the digital signature can be verified by using the public key listed in the Digital Signature Certificate issued to that person;
- (f) That the standards referred to in rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 have been complied with, in so far as they relate to the creation, storage and transmission of the digital signature; and
- (g) That the digital signature is linked to the electronic record in such a manner that if the electronic record was altered the digital signature would be invalidated.

**BLOCKING OF WEBSITES**  
**MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY**  
**(Department of Information Technology)**  
**ORDER**  
**New Delhi, 7th July, 2003**

**Subject: Procedure for Blocking of Websites**

As per the Gazette Notification (Extraordinary) No. G.S.R. 181(E), dated 27th February, 2003, published in part II, section 3, Sub-section (i), Indian Computer Emergency Response Team (CERT-In) has been designated as the single authority for issuing of instruction in the context of blocking of websites. CERT-In has to instruct the Department of Telecommunication to block the website after,

- (i) Verifying the authenticity of the complaint
- (ii) Satisfying that action of blocking of websites is absolutely essential.

II. The blocking of websites may be the need of several agencies engaged in different walks of public and administrative lives due to a variety of reasons. Explicit provision for blocking of the websites in the Information Technology Act, 2000 is available only in section 67, relating to pornographic content on the website. In addition, section 69 empowers the Controller of Certifying Authorities to intercept any information transmitted through any computer resource in relation only to the following five purposes:-

- (i) Interest of the sovereignty or integrity of India,
- (ii) The security of the State,
- (iii) Friendly relations with foreign States, or
- (iv) Public order, or
- (v) For preventing incitement to the commission of any cognizable offence.

III. As already noted there is no explicit provision in the Information Technology Act, 2000 for blocking of websites. In fact, Blocking is taken to amount to censorship. Such Blocking can be challenged if it amount to restriction of freedom of speech and expression. But websites promoting hate content slander or defamation of others, promoting gambling, promoting racism, violence and terrorism and other such material, in addition to promoting pornography, including child pornography, and violent sex can reasonable be blocked since all such websites may not claim constitutional right to free speech. Blocking of such websites may be equated to “balanced flow of information” and not censorship.

IV. The websites promoting the abovementioned types of content, not covered under Freedom of Speech may need to be blocked under the inherent powers of the Government, “to the extent of executive authority read with legal powers vested in Central Government and Controller under various provisions of various laws”.

V. The detailed procedure for submitting a complaint to the Director, CERT-In for blocking of a website shall be as follows:-

1. The following officers listed in Para 2 of the Gazette Notification can submit the complaint to the Director, CERT-In:-

- (i) Secretary, National Security Council Secretariat (NSCS);
- (ii) Secretary, Ministry of Home Affairs, Government of India;
- (iii) Foreign Secretary in the Department of External Affairs or a representative not below the rank of joint Secretary;
- (iv) Secretaries, Department of Home Affairs of each of the States and of the Union territories;
- (v) Central Bureau of Investigation (CBI), Intelligence Bureau (IB), Director General of police of all the state and such other enforcement agencies;
- (vi) Secretaries or Heads of all the Information Technology Department of all the states and Union Territories not below the rank of Joint Secretary of Central Government;
- (vii) Chairman of the National Human Rights Commission or Minorities Commission or Scheduled Castes or Scheduled Tribes Commissions or National Women Commission.
- (viii) The directive of the Courts;
- (ix) Any others as may be specified by the Government.

2. The complaint shall contain the following:-

- (i) Name of the complainant with address, telephone number, fax number, and e-mail.
- (ii) The address of the offending website.

- (iii) The name of the organization with address, if known, which is promoting / hosting the website.
- (iv) Specific reasons for requesting blocking of website. This may be from any of the following:-

Promoting hate content, slander or defamation of others, promoting, gambling, promoting racism, violence and terrorism and other such material, promoting pornography, including child pornography and violent sex.

- (v) Any other reasons may be specified by the complainant.
- (vi) Segment of population or the audience that is adversely affected by the offending website.

3. The complaint may be submitted in writing by an authorised officer of the above named organisation on the letter head. This can be sent either by mail or by fax or by e-mail digitally signed.

4. Each complaint shall be assigned a complaint number and recorded in a register along with the time and date of the receipt.

5. CERT-In staff shall verify that the complainant belongs to one of the organisations that have been listed above. If needed, this will be verified telephonically from the concerned office.

6. Each complaint shall be acknowledged to the complaint within 24 hours of its receipt.

7. In the case of complaints received by fax and e-mail which is not digitally signed, the complainant shall be required to provide an ink-signed copy of the complaint by fax or e-mail. The processing of the complaint shall begin without waiting for the receipt of the ink- signed copy.

8. Director, CERT-In will assign the complaint to a technical expert to view the said website and print the offending content as a sample within a day of the receipt of the complaint.

9. The complaint along with the printed sample content of the website shall be examined by a duly constituted committee under the Chairmanship of Director, CERT-In with representatives of DIT and Law Ministry / Home Ministry. The committee will meet within a day of the complaint and the content being notified by Director, CERT-In to the members of the Committee. It will meet and take on the spot decision on whether the website is to be blocked or not.

10. The decision on blocking of the website by the Committee along with the complaint and details thereof shall be submitted by Director, CERT-In to the Additional Secretary, DIT for the approval of the Secretary, DIT.

11. On receipt of the approval from DIT, Director, CERT-In will issue instruction to DOT for blocking of website.

12. The entire exercise shall be completed within seven working days of the receipt of a complaint.

13. In case of an emergency situation, to be decided by Director, CERT-In in consultation with the Additional Secretary, DIT, instructions for blocking of website will be immediately issued by Director, CERT-In to Dot.

14. Strict confidentiality shall be maintained by CERT-In regarding all the complaints as also their processing.

15. The Director, CERT-In shall maintain complete record, in electronic database as also in paper files/registered, of the cases of blocking of website processed. This database shall be the property of the DIT and shall not be used for any commercial purpose.

16. The Director, CERT-In shall submit a monthly report of the cases of blocking of the website processed in each month, by 7th of the next month (or the next working day if 7th happens to be a holiday) to the Additional Secretary, DIT.

17. The Director CERT-In shall arrange to make available, the record of the cases of blocking of the website processed by CERT-In, as and when required for audit by an officer designated by secretary, DIT for this purpose. This inspection/ audit may be undertaken on a quarterly basis.

18. The service for blocking of the websites containing offending material is to be provided by CERT-In in public interest and hence no fees shall be charged for providing this service.

## **THE CYBER APPELLATE TRIBUNAL (SALARY, ALLOWANCE AND OTHER TERM AND CONDITION OF SERVICE OF CHAIRPERSON AND MEMBERS RULES, 2009**

*In exercise of the powers conferred by clause (r) of sub-section (2) of Section 87, read with section 52 of the Information Technology Act 2000 (21 of 2000), and in suppression of the cyber regulation Appellate Tribunal (Salary, Allowance And Other Term And Condition Of Service Of Presiding Officer) Rules, 2003 except as respect thing done or omitted to be done before such suppression, the Central Government hereby makes the following rules regulating the terms and conditions of the service of the Chairperson and Members of the Cyber Appellate Tribunal, namely:-*

### **1. Short title and commencement:-**

(1) These rules may be called the CYBER APPELLATE TRIBUNAL (SALARY, ALLOWANCES AND OTHER TERMS AND CONDITIONS OF SERVICE OF CHAIRPERSON AND MEMBERS) RULES, 2009.

(2) They shall come into force on the date of their publications in the Official Gazette

### **2. Definitions: -**

(1) In these rules, unless the context otherwise requires-

- (a) "Act" means Information Technology Act 2000, as amended by the Information Technology (Amendment) Act, 2008;
- (b) "Cyber Appellate Tribunal" means Cyber Appellate Tribunal established under sub-section (1) of section 48 of the Act;
- (c) "Chairperson" means a person appointed as Chairperson of a Cyber Appellate Tribunal under section 49 of the Act; (d)
- (d) "Member" means a person appointed as Member of a Cyber Appellate Tribunal under section 49 of the Act;

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

### **3. Salary and Allowances: -**

(1) The Chairperson and Members shall be paid such salary and allowances, as admissible to a Secretary to the Government of India, including all the benefits that a Secretary is entitled to:

Provided that in the case of appointment of a person as Chairperson or Member, as the case may be, who has retired as a Judge of a Supreme Court or a High Court or who has retired from service under the Central Government or a State Government and who is in receipt of, or has received, or has become entitled to receive any retirement benefits by way of pension, gratuity, employer's contribution to contributory Provident Fund or other forms of retirement benefits, the pay of such Chairperson or the Member as the case may be, shall be reduced by the gross amount of pension or employer's contribution to the contributory Provident Fund or any other form of retirement benefit, if any, drawn or to be drawn by him:

Provided further that in case a retired Judge of a Supreme Court or a High Court is appointed as Chairperson or Member, as the case may be, the terms and conditions of service of such Chairperson or Member shall be in accordance with the instructions issued by the Ministry of Finance in respect of appointment of Judges to various Tribunals and in consultation with that Ministry.

### **4. Leave: -**

The Chairperson and Members in Cyber Appellate Tribunal shall be entitled to leave as applicable to the Secretary to the Government of India in respect of Earned Leave, Half Pay Leave, Extra Ordinary Leave, Commutation of Leave and Casual Leave etc.

### **5. Leave Sanctioning Authority: -**

The Secretary, Department of Information Technology, Ministry of Communications & Information Technology, Government of India, shall be the authority competent to sanction leave to the Chairperson and the Members.

### **6. Pension or Provident Fund: -**

(1) In case a serving Judge of a Supreme Court or a High Court or a member of the Indian Legal Service is appointed to the post of Chairperson or the Member, the service rendered in Tribunal shall count for pension, to be drawn in accordance with the rules of the service to which he belongs, and he shall also be governed by the provisions of the General Provident Fund (Central Services) Rules, 1960.

(2) In all other cases, the Chairperson and Member shall be governed by the provision of the Provident Fund (India) Rules, 1962.

**7. Travelling Allowances: -**

The Chairperson or the Member as the case may be, while on tour (including the journey undertaken on the expiry of his term with the Cyber Appellate Tribunal to proceed to his home town) shall be entitled to the travelling allowance, daily allowances, transportation of personal effects and other similar matters at the same rates as are applicable to Secretary to the Government of India.

**8. Leave Travel Concession: -**

The Chairperson or Member shall be entitled to avail leave travel concession at the same rate as are admissible to the Secretary to the Government of India.

**9. Facility of Conveyance: -**

The Chairperson or Member shall be entitled to hire a Taxi on whole time basis in accordance with the rules or orders for the time being in force for hire of taxi by a Secretary to the Government of India.

**10. House Rent Allowance: -**

The Chairperson and Member shall be entitled to house rent allowance at the same rate as are, for the time being, admissible to Group 'A' officers of the Central Government drawing equivalent pay and grade pay.

**11. Facilities for medical treatment: -**

The Chairperson and Member shall be entitled to medical treatment and hospital facilities, as provided in the Central Government Health Scheme Rules, 1954 and in places where the Central Government Health Scheme is not in operation, the said Chairperson and Member shall be entitled to the facilities as provided in the Central Services (Medical Attendance) Rules, 1944.

**12. Oath of office and secrecy.-**

Every person appointed as the Chairperson or the Member, as the case may be, shall, before entering upon his office, make and subscribe an oath of office and secrecy, in form I and form II respectively annexed to these rules.

**13. Declaration of financial or other interest.-**

Every person, on his appointment as the Chairperson or the Member, as the case may be, shall give a declaration in form III annexed to these rules, to the satisfaction of the Central Government, that he does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or the Member, as the case may be.

**14. Residuary provision.-**

Any matter relating to the conditions of services of the Chairperson and Member with respect to which no express provision has been made in these rules shall be as per rules applicable to the Group 'A' officers of the Central Government drawing equivalent pay and grade pay.

**FORM I**  
**(see rule 12)**

**FORM OF OATH OF OFFICE FOR THE CHAIRPERSON /MEMBERS OF THE CYBER  
APPELLATE TRIBUNAL**

I, ....., having been appointed as the Chairperson / Member (*cross out portion not applicable*) do solemnly “affirm and do swear in the name of god that I will faithfully and consciously discharge my duties as the Chairperson / Member (*cross out portion not applicable*), of the Cyber Appellate Tribunal, to the best of my ability, knowledge and judgment, without fear of favour, affection or ill-will.

Dated .....  
Place.....

Name of the Chairperson/Member  
CYBER APPELLATE TRIBUNAL

**FORM II**  
**(see rule 12)**

**FORM OF OATH OF SECRECY FOR THE CHAIRPERSON /MEMBERS OF THE CYBER  
APPELLATE TRIBUNAL**

I, ....., having been appointed as the Chairperson / Member (*cross out portion not applicable*) do solemnly “affirm and do swear in the name of god that I will not directly or indirectly communicate or reveal to any person or persons any matter which shall be brought under my consideration or shall become known to me as the Chairperson / Member (*cross out portion not applicable*), of the Cyber Appellate Tribunal except as may be required for the due discharge of my duties as the Chairperson / Member (*cross out portion not applicable*)

Dated .....  
Place.....

Name of the Chairperson/Member  
CYBER APPELLATE TRIBUNAL

**FORM III**  
**(see rule 13)**

**DECLARATION AGAINST ACQUISITION OF ANY ADVERSE FINANCIAL OR OTHER  
INTEREST**

I, ....., having been appointed as the Chairperson / Member (*cross out portion not applicable*) Cyber Appellate Tribunal, do solemnly “affirm and declare that I do not shall have in future any financial or other interest which is likely to affect prejudicially my functioning as Chairperson / Member (*cross out portion not applicable*), of the Cyber Appellate Tribunal.

Dated .....  
Place.....

Name of the Chairperson/Member  
CYBER APPELLATE TRIBUNAL

## **THE CYBER APPELLATE TRIBUNAL (PROCEDURE FOR INVESTIGATION OF MISBEHAVIOR IN CAPACITY OF CHAIRPERSON AND MEMBERS) RULES, 2009**

*In exercise of the powers conferred by clause (s) of sub section (2) of section 87, read with subsection (3) of section 54 of the Information Technology Act 2000 (21 of 2000) and in suppression of the Cyber Regulation Appellate Tribunal (procedure for Investigation of misbehaviour or incapacity of Presiding Officer) Rules, 2003, except as respects things done or omitted to be done before such suppression, Central Government hereby makes the following rules, namely -*

### **1. Short title and commencement**

(1) These rules may be called THE CYBER APPELLATE TRIBUNAL (PROCEDURE FOR INVESTIGATION OF MISBEHAVIOR OR INCAPACITY OF CHAIRPERSON AND MEMBERS) RULES, 2009.

(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 requires -

- (a) "Act" means the Information Technology Act 2000, (21 of 2000);
- (b) "Chairperson" means the as Chairperson of a Cyber Appellate Tribunal under section 49 of the Act;
- (c) "Committee" means a Committee constitute under sub-rule (2) of Rule 3;
- (d) "Member" means the Cyber Appellate Tribunal appointed under section 49 of the Act;
- (e) "Tribunal" means the Cyber Appellate Tribunal established under sub-section (1) of section 48 of the Act;

(2) All other words and expressions used but not defined in these rules shall have the meaning respectively assigned to them in the Act.

### **3. Committee for investigation of complaints.-**

(1) If a written complaint, alleging any definite charges of misbehavior or incapacity to perform the functions of the offices in respect of a Chairperson or Member, is received by the Central Government, it shall make a preliminary scrutiny of such complaint.

(2) If on preliminary scrutiny, the Central Government considers it necessary to investigate into the allegation, it shall place the complaint together with other material as may be available, before a Committee consisting of the following officers to investigate the charges of allegations made in the complaint, namely:-

- (i) the Secretary (Co-ordination and Public Grievances), in the Cabinet Secretariat, Government of India - Chairman;
- (ii) the Secretary, Department of Information Technology, Government of India – Member;
- (iii) the Secretary, Department of Legal Affairs, Ministry of Law and Justice, Government of India - Member.

(3) The Committee shall devise its own procedure and method of investigation, which may include recording of evidence of the complainant and collection of material under rule 4, which may be relevant to the conduct of inquiry.

(4) The Committee shall submit its findings to the President as early as possible within a period that may be specified by the President in this behalf.

### **4. Judge to conduct inquiry**

(1) If the President, on receipt of the report of the Committee under sub-rule (4) of rule 3, is of the opinion that there are reasonable grounds for making an inquiry into the truth of any imputation of misbehavior or incapacity of a Chairperson or the Member, as the case may be, then, he shall make a reference to the Chief Justice of India requesting him to nominate a Judge of the Supreme Court to conduct the inquiry.

(2) The President shall, by order, appoint the Judge of the Supreme Court nominated by the Chief Justice of India (hereinafter referred to as Judge) for the purpose of conducting the inquiry.

(3) Notice of appointment of a Judge under sub-rule (2) shall be given to the Chairperson or Member, as the case may be.

(4) The President shall forward to the Judge a copy of-

- (a) the articles of charges against the Chairperson or the Member as the case may be, and the statement of imputations;
- (b) the statement of witnesses, if any; and
- (c) material documents relevant to the inquiry.

(5) The Judge appointed under sub-rule (2) shall complete the inquiry within such time or further time as may be specified by the President.

(6) The Chairperson or the Member, as the case may be, concerned shall be given a reasonable opportunity of presenting a written statement of defence within such time as may be specified in this behalf by the Judge.

(7) Where it is alleged that the Chairperson or the Member, as the case may be, concerned is unable to discharge the duties of his office efficiently due to any physical or mental incapacity and the allegation is denied, the Judge may arrange for the medical examination of the Chairperson or the Member, as the case may be, by such Medical Board as may be appointed for the purpose by the President and the Chairperson or Member concerned, as the case may be, shall submit himself to such medical examination within the time specified in this behalf by the Judge.

(8) The Medical Board shall undertake such medical examination of the Chairperson or the Member, as the case may be, as may be considered necessary to and submit a report to the Judge stating therein whether the incapacity is such as to render the Chairperson or the Member, as the case may be, unfit to continue in office.

(9) If the Chairperson or the Member, as the case may be, refuses to undergo such medical examination as considered necessary by the Medical Board, the Board shall submit a report to the Judge stating therein the examination which the Chairperson or Member has refused to undergo, and the Judge may, on receipt of such report, presume that the Chairperson or the Member, as the case may be, suffers from such physical or mental incapacity as is alleged in the article of charges referred to clause (a) of sub-rule (4).

(10) The Judge may, after considering the written statement of the Chairperson or the Member, as the case may be, and report of the Medical Board, if any, amend the charges referred to in clause (a) of sub-rule (4) and in such case, the Chairperson or Member shall be given a reasonable opportunity of presenting a fresh written statement of defence.

(11) The Central Government shall appoint an officer of that Government or an advocate to present the case against the Chairperson or the Member, as the case may be, before the Judge.

(12) Where the Central Government has appointed an advocate to present its case before the Judge, the Chairperson or the Member, as the case may be, concerned shall also be allowed to present his case by an advocate chosen by him.

## **5. Application of the Departmental Inquiries (Enforcement of Witness and Production of Documents) Act, 1972 to inquiries under these rules. -**

The provisions of the Departmental Inquiries (Enforcement of Witness and Production of Documents) Act, 1972 (18 of 1972), shall apply to the inquiries made under these rules as they apply to departmental inquiries.

## **6. Powers of Judge**

The Judge shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and shall have power to regulate his own procedure including the fixing of places and times of his inquiry.

## **7. Suspension of Chairperson or Member.-**

Notwithstanding anything contained in Rule 4 and without any prejudice to any action being taken in accordance with the said rule, the President, keeping in view the gravity of charges may suspend the Chairperson or the Member, as the case may be, of the Tribunal against whom a complaint is under investigation or inquiry.

## **8. Subsistence allowance**

The payment of subsistence allowance to a Chairperson or the Member, as the case may be, under suspension shall be regulated in accordance with the rules and orders for the time being applicable to a Secretary to the Government of India belonging to the Indian Administrative Service.

## **9. Inquiry Report**

After the conclusion of the investigation, the Judge shall submit his report to the President stating therein his findings and the reasons therefore on each of the articles of charges separately with such observations on the whole case as he thinks fit.

## **THE INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARD FOR INTERCEPTION, MONITORING AND DECRYPTION OF INFORMATION) RULES, 2009**

*G.S.R. 780 (E).- In exercise of the powers conferred by clause (y) of sub-section (2) of section 87 read with sub-section (2) of section 69 of the Information Technology Act 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:*

### **1. Short title and commencement-**

- (1) These rules may be called the Information Technology (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009.
- (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 requires,-

- (a) "Act" means the Information Technology Act, 2000 (21 of 2000);
- (b) "Communication" means dissemination, transmission, carriage of information or signal in some manner and include both a direct communication and an indirect communication;
- (c) "Communication link" means the use of satellite, microwave, radio, terrestrial line, wire, wireless or any other communication media to inter-connect computer resource;
- (d) "Competent authority" means-
  - (i) the secretary in the Ministry of Home Affairs, in case of the Central Government; or
  - (ii) the Secretary in charge of the Home Department, in case of a State Government or Union territory as the case may be;
- (e) "decryption" means the process of conversion of information in non-intelligible form to an intelligible form via a mathematical formula, code, password or algorithm or a combination thereof;
- (g) "decryption assistance" means any assistance to –
  - (i) allow access, to the extent possible, to encrypted information; or
  - (ii) facilitate conversion of encrypted information into an intelligible form;
- (h) "decryption direction" means a direction issued under rule 3 in which a decryption key holder is directed to -
  - (i) disclose a decryption key; or
  - (ii) provide decryption assistance in respect of encrypted information
- (i) "decryption key" means any key, mathematical formula, code, password, algorithm or any other data which is issued to-
  - (i) allow access to encrypted information; or
  - (ii) facilitates the conversion of encrypted information into an intelligible form;
- (j) "decryption key holder" means any person who deploys the decryption mechanism and who is in possession of a decryption key for purpose of subsequent decryption of encrypted information relating to direct or indirect communications;
- (k) "information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;
- (l) "intercept" with its grammatical variations and cognate expressions, means the rural or other acquisition of the content of any information through the use of any means, including an interception device, so as to make some or all of the contents of a information available to a person other than the sender or recipient or intended of that communication, and includes-
  - (a) monitoring of any such information by means of a monitoring device;
  - (b) viewing, examination or inspection of the contents of any direct or indirect information; and
  - (c) diversion of any direct or indirect information from its intended designation to any other destination;
- (m) "interception device" means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself in combination with any other instrument, device, equipment or apparatus, to intercept any information; and any reference to an "Interception device" includes where applicable, a reference to a "monitoring device";
- (n) "intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;
- (o) "monitor" with its grammatical variations and cognate expressions, includes to view or to inspect or to listen to or record any information by means of a monitoring device;

- (p) "monitoring device" means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument, device, equipment or apparatus which used or can be used, whether by itself in combination with any other instrument, device, equipment or apparatus, to view or to inspect or to or record any information;
- (q) "Reviewing Committee" means the Review Committee constituted under rule 419A of Indian Telegraph Rules, 1951.

### **3. Direction for Interception or monitoring or Decryption of Information.-**

No person shall carry out the Interception or monitoring or decryption of information generated, transmitted, received or stored in any computer resource under sub-section (2) of section 69 of the Act, except by an order issued by the competent authority.

Provided that in an unavoidable to the Government of India, who has been duly authorizes by the competent authority:

Provided further that in case of emergency-

(i) in remote areas, where obtaining of prior directions for interception or monitoring or decryption of information is not feasible; or

(ii) for operational reasons where obtaining of prior directions for interception or monitoring or decryption of information generated, transmitted, received or stored in any computer resource is not feasible,

the interception or monitoring or decryption of information generated, transmitted, received or stored in any computer resource may be carried out with the prior approval of the Head or second senior most officer of the security and law enforcement agency (hereinafter referred to as the said security agency) at the Central level and the officer authorised in this behalf, not below the rank of the inspector General of Police or an officer of equivalent rank, at the State or Union territory level:

Provided also that the officer, who approved such interception or monitoring or decryption of information in case of emergency, shall inform in writing to the competent authority about the emergency and of such interception or monitoring or decryption within three working days and obtain the approval of the competent authority thereon within a period of seven working days and if the approval of competent authority is not obtained within the said period of seven working days, such interception or monitoring or decryption shall cease and the information shall not be interception or monitoring or decrypted thereafter without the prior approval of the competent authority.

### **4. Authorisation of agency of Government-**

The competent authority may authorize an agency of the Government to intercept, monitor or decrypt information generated, transmitted, received or stored in any computer resource for the purpose specified in sub-section (1) of the section 69 of the Act.

### **5. Issue of decryption direction by competent authority.-**

The competent authority may, under rule 3 give any decryption direction to the decryption key holder for decryption of nay information involving a computer resource or part thereof.

### **6. Interception or monitoring or decryption of information by a state beyond its jurisdiction.-**

Notwithstanding anything contained in rule 3, if a State Government or Union territory Administration requires any interception or monitoring or decryption of information beyond its territorial jurisdiction, the Secretary in-charge of the Home Department in that State or Union territory, as the case may be, shall make a request to the Secretary in the Ministry of Home affairs, Government of India for issuing direction to the appropriate authority for such interception or monitoring or decryption of information.

### **7. Content of direction.-**

Any direction issued by the competent authority under rule 3 shall contain reason for such direction and a copy of such direction shall be forwarded to the Review Committee within a period of seven working days.

### **8. Competent authority to consider alternative means in acquiring information.-**

The competent authority shall, before issuing any direction under rule 3, consider possibility of acquiring the necessary information by other means and the direction under rule 3 shall be issued only when it is not possible to acquire the information by any other reasonable means.

### **9. Direction of interception or monitoring or decryption of any specific information.-**

The direction of interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource shall be of any information as is sent to or from any person or class of persons

or relating to any particular subject whether such information or class of information are received with one or more computer resource, or being computer resource likely to be used for the generation, transmission, receiving, storing of information from or to one particular person or one or many set of premises, as may be specified or described or described in the direction.

**10. Direction to specify the time and designation of the officer to whom information to be disclosed-**

Every directions under rule 3 shall specify the name and designation of the officer of the authorized agency to whom the intercepted or monitored or decrypted or stored information shall be disclosed and also specify that the use of intercepted or monitored or decrypted information shall be subject to the provisions of sub-section (1) of section 69 of the said Act.

**11. Period within which direction shall remain in force.-**

The direction for interception or monitoring or decryption shall remain in force, unless revoked earlier for a period not exceeding sixty days from the date of its issue and may be renewed from time to time for such period not exceeding the total period of one hundred and eighty days.

**12. Authorised agency to designate nodal officer.-**

The agency authorized by the competent authority under rule 4 shall designate one or more nodal officer, not below the rank of Superintendent of Police or Additional Superintendent of Police or the officer of the equivalent rank, to authenticate and send the requisition conveying direction issued under rule 3 for interception or monitoring or decryption to the designated officer of the concerned intermediaries or person in-charge of computer resource:

Provided that an officer, not below the rank of Inspector of Police or officer of equivalent rank, shall deliver the requisition to the designated officer of the intermediary.

**13. Intermediary to provide facilities, etc.-**

(1) The officer issuing the requisition conveying direction issued under rule 3 for interception or monitoring or decryption of information shall also make a request in writing to the designated officers of intermediary or person in-charge of computer resources, to provide all facilities, co-operation and assistance for interception or monitoring or decryption mentioned in the directions.

(2) On the receipt of request under sub-rule (1), the designated officers of intermediary or person in-charge of computer resources, shall provide all facilities, co-operation and assistance for interception or monitoring or decryption of information mentioned in the direction.

(3) Any direction of decryption of information issued under rule 3 to intermediary shall be limited to the extent the information is encrypted by the intermediary or the intermediary has control over the decryption key.

**14. Intermediary to designate officers to receive and handle requisition.-**

Every intermediary in-charge of computer resource shall designate an officer to receive requisition, and another officer to handle such requisition from the nodal officer for interception or monitoring or decryption of information generated, transmitted, received or stored in any computer resource.

**15. Acknowledgement of instruction.-**

The designated officer of the intermediary or person in-charge of computer resources shall acknowledge the instructions received by him through letters or fax or e-mail signed with electronic signature to the nodal officer of the concerned agency within two hours on receipt of such intimation or direction for interception or monitoring or decryption of information.

**16. Maintenance of records by designated officer.-**

The designated officer of intermediary or person in-charge of computer resource authorized to intercept or monitor or decrypt any information shall maintain proper records mentioning therein, the intercepted or monitored or decrypted information, the particulars of persons, computer resource, e-mail account, website address, etc. whose information has been intercepted or monitored or decrypted, the name and other particulars of the officer or the authority to whom the intercepted or monitored or decrypted information has been disclosed, the number of copies, including corresponding electronic record of the intercepted or monitored or decrypted information made and the mode or the method by which such copies, including corresponding electronic record are made the date of destruction of the copies, including corresponding electronic record and the duration within the directions remain in force.

**17. Decryption key holder to disclose decryption key or provide decryption assistance.-**

If a decryption direction or a copy thereof is handled to the decryption key holder to whom the decryption direction is addressed by the nodal officer referred to in rule 12, the decryption key holder shall within the period mentioned in the decryption direction-

- (a) disclose they decryption key; or
- (b) provide the decryption assistance,

Specified in the decryption direction to the concerned authorized person.

**18. Submission of list of interception or monitoring or decryption of information.-**

(1)The designated officer of the intermediary or person in-charge of computer resources shall forward in every fifteen days a list of interception or monitoring or decryption authorizations received by them during the preceding fortnight to the nodal officers of the agencies authorized under rule 4 for confirmation of the authenticity of such authorizations.

(2)The list referred to in sub-rile (1) shall includes detail, such as the reference and date of orders of the concerned competent authority including any order issued emergency cases, date and time of receipt of such order and the date and time of implementation of such order.

**19. Intermediary to ensure effective check in handling matter of interception or monitoring or decryption of information.-**

The intermediary or the person in-charge of the computer resource so directed under rule 3, shall provided technical assistance and the equipment including hardware, software, firmware, storage, interface and access to the equipment wherever requested by the agency authorized under rule 4 for performing interception or monitoring or decryption including for the purpose of –

- (i) the installation of equipment of the agency authorized under rule 4 for the purposes of interception or monitoring or decryption or accessing stored information in accordance with directions by the nodal officer; or
- (ii) the maintenance, testing or use of such equipment; or
- (iii) the removal of such equipment; or
- (iv) the performance of nay action required for accessing of stored information under the direction issued by the competent authority under rule 3.

**20. Intermediary to ensure effective check in handling matter of interception or monitoring or decryption of information.-**

The intermediary or person in-charge of computer resources shall put in place adequate and effective internal checks to ensure the unauthorized interception of information does not take place and extreme secrecy is maintained and utmost care and precaution shall be taken in the matter of interception or monitoring or decryption of information as it affects privacy of citizens and also that it is handles only by the designated officers of the intermediary and no other person of the intermediary or person in-charge of computer resources shall have access to such intercepted or monitored or decrypted information.

**21. Responsibility of intermediary.-**

The intermediary or person in charge of computer resources shall be responsible for any action of their employees also and in case of violation pertaining to maintenance of secrecy and confidentiality of information or any unauthorized interception or monitoring or decryption of information, the intermediary or person in-charge of computer resources shall be liable for nay action under the relevant provisions of the laws for the time being in force.

**22. Review of directions of competent authority.-**

The review committee shall meet at least once in two months and record its finding whether the directions issued under rule 3 are in accordance with the provisions of sub-section (2) of section 69 of the Act and where the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above, it may set aside the directions and issue order for destruction of the copies, including corresponding electronic record of the intercepted or monitored or decrypted information.

**23. Destruction of record of interception or monitoring or decryption of information.-**

(1) Every record, including electronic records pertaining to such directions for interception or monitoring or decryption of information and of intercepted or monitored or decrypted information shall be destroyed by the

security agency in every six months except in a case where such information is required, or likely to be required for functional requirements.

(2) Save as otherwise required for the purpose of any ongoing investigation, criminal complaint or legal proceeding, the intermediary or person in-charge of computer resource shall destroy records pertaining to directions for interception of information within a period of two months of discontinuance of the interception or monitoring or decryption of such information and in doing so they shall maintain extreme secrecy.

#### **24. Prohibition of interception or monitoring or decryption of information without authorization.-**

(1) Any person who intentionally or knowingly, without authorization under rule 3 or rule 4, intercepts or attempts to intercept, or authorizes or assists any other person to intercept or attempts to intercept any information in the course of its occurrence or transmission at any place within India, shall be proceeded against and published accordingly under the relevant provisions of the laws for the time being in force.

(2) Any interception, monitoring or decryption of information in computer resource by the employee of an intermediary or person in-charge of computer resource or a person duly authorized by the intermediary, may be undertaken in course of his duty relating to the services provided by that intermediary, if such activities are reasonably necessary for the discharge his duties as per the prevailing industry practices, in connection with the following matters, namely-

- (i) installation of computer resource or any equipment to be used with computer resource; or
- (ii) operation or maintenance of computer resource; or
- (iii) installation of any communication link or software either at the end of the intermediary or subscriber or installation of user account on the computer resource of intermediary and testing of the same for its functionality;
- (iv) accessing stored information from computer resource relating to the installation, connection or maintenance of equipment, computer resource or a communication link or code; or
- (v) Accessing stored information from computer resource for the purpose of-
  - a. implementing information security practices in the computer resource;
  - b. determining any security breaches, computer contaminant or computer virus;
  - c. undertaking forensic of the concerned computer resource as a part of investigation; or
- (vi) accessing or analyzing information from a computer resource for the purpose of tracing a computer resource or any person who has contravened, or is suspected of having contravened or being likely to contravene, any provision of the Act that is likely to have an adverse impact on the services provided by the intermediary.

(3) The intermediary or the person in-charge of computer resource and its employees shall maintain strict secrecy and confidentiality of information while performing the actions specified under sub-section (2).

#### **25. Prohibition of disclosure of intercepted or monitored or decrypted information.-**

(1) The content of intercepted or monitored or stored or decrypted information shall not be used or disclosed by intermediary or any of its employees or person in-charge of computer resource to any person other than the intended recipient of the said information under rule 10.

(2) The content of intercepted or monitored or decrypted information shall not be used or disclosed by the agency authorised under rule 4 for any other purpose, except for investigation or sharing with other security agency for the purpose of investigation or in judicial proceeding before the competent court in India.

(3) Save as otherwise provided in sub-rule (2), the content of intercepted or monitored or decrypted information shall not be disclosed or reported in public by any means, without the prior order of competent court in India.

(4) Save as otherwise provided in sub-rule (2), strict confidentiality shall be maintained in respect of direction for interception, monitoring or decryption issued by concerned competent authority or the nodal officers.

(5) Any intermediary or its employees or person in-charge of computer resource who contravenes provisions of these rules shall be proceeded against and published accordingly under, the relevant provisions of the Act for the time being in force.

(6) Whenever asked for by the concerned security agency at the Centre, the security agencies at the State and the Union territory level shall promptly share any information which they may have obtained following directions for interception, monitoring or decryption of any information generated, transmitted, received or stored in any computer resource under rule 3, with the security agency at the Centre.

## **THE INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARD FOR BLOCKING FOR ACCESS OF INFORMATION BY PUBLIC) RULES, 2009**

*G.S.R. 781 (E).- In exercise of the powers conferred by clause (z) of sub-section (2) of section 87 read with sub-section (2) of section 69A of the Information Technology Act 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:*

### **1. Short title and commencement-**

(1) These rules may be called the Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) Rules, 2009.

(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 requires,-

- (a) "Act" means the Information Technology Act, 2000 (21 of 2000);
- (b) "Computer resource" means computer resource as defined in the clause (k) of sub-section (1) of section 2 of the Act;
- (c) "Designated Officer" means an officer designated as Designated Officer under rule 3;
- (d) "Form" means a form appended to these rules;
- (e) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;
- (f) "nodal officer" means the nodal officer designated as such under rule 4;
- (g) "Organisation" means-
  - (i) state Government and Union territories;
  - (ii) any agency of the Central Government, as may be notified in the official gazette, by the Central Government.
- (h) "request" means the request for blocking of access by the public any information generated transmitted, received, stored or hosted in any computer resource;
- (i) "Review Committee" means the review committee constituted under rule 419A of Indian Telegraph Rules, 1951.

### **3. Designated Officer.-**

The Central Government shall designate by notification in official gazette, an officer of the Central Government not below the rank of joint secretary, as the "designated Officer", for the purpose of issuing direction for blocking for access by the public any information generated transmitted, received, stored or hosted in any computer resource under sub-section (2) of section 69A of the Act.

### **4. Nodal officer of organization.-**

Every organization for the purpose of these rules, shall designate one of its officer as the Nodal Officer and shall initiate the same to the Central Government in the Department of Information Technology under the Ministry of Communication and Information Technology, Government of India and also publish the name of the said Nodal Officer on their website.

### **5. Direction by Designated Officer.-**

The Designated Officer may, on receipt of any request from the Nodal Officer of an organization or a competent court, by order direct any Agency of the Government or intermediary to block for access by the public any information or part thereof generated, transmitted, received, stored or hosted in any computer resource for any of the reason specified in sub-section (1) of section 69A of the Act.

### **6. Forwarding of request by organization.-**

(1) Any person may send their complaint to the Nodal Officer of the concerned organization for blocking by the public any information generated transmitted, received, stored or hosted in any computer resource.

Provided that any request, other than the one from the Nodal Officer of the organization, shall be sent with the approval of the Chief Secretary of the concerned State or Union territory to the Designated Officer:

Provided further that in case a Union territory has no Chief Secretary, then, such request may be approved by the Adviser to the Administrative of that Union territory.

(2) The organisation shall examine the complaint received under sub-rule (1) to satisfy themselves about the need for taking of action in relation to the reasons enumerated in sub-section (1) of section 69A of the Act and after being satisfied, it shall send the request through its nodal officer to the Designated Officer in the format specified in the form appended to these rules.

(3) The Designated Officer shall not entertain any complaint or request for blocking of information directly from any person.

(4) The request shall be in writing on the letter head of the respective organisation, complete in all respects and may be sent either by mail or by fax or by e-mail signed with electronic signature of the Nodal Officer.

Provided that in case the request sent either by fax or by e-mail which is not signed with electronic signature of the Nodal Officer shall provide a signed copy of the request so as to reach the Designated Officer within a period of three days of receipt of the request by such fax or e-mail.

(5) On receipt each request shall be assigned a number alongwith the date and time of its receipt by the Designated Officer and he shall acknowledge the receipt thereof to the Nodal Officer within a period of twenty four days of its receipt.

### **7. Committed for examination of request.-**

The request alongwith the printed sample content of the alleged offending information or part thereof shall be examined by a committee consisting of the Designated Officer as its chairperson and representatives, not below the rank of Joint Secretary in Ministries of Law and Justice, Home Affairs, Information and Broadcasting and the Indian Computer Emergency Response Team appointed under sub-section (1) of section 70B of the Act.

### **8. Examination of request.-**

(1) On receipt of request under rule 6, the Designated Officer shall make all reasonable efforts to identify the person or intermediary who has hosted the information or part thereof as well as the computer resource on which such information or part thereof is being hosted and where he is able to identify such person or intermediary and the computer resource hosting the information or part thereof which have been requested to be blocked for public access, he shall issue a notice by way of letters or fax pr e-mail signed with electronic signatures to such person or intermediary in control of such computer resource to appear and submit their reply and clarifications if any, before the committee referred to in rule 7, at a specified date and time, which shall not be less than forty-eight hours from the time of receipt of such notice by such person or intermediary.

(2) In case of non-appearance of such person or intermediary, who has been served with the notice under sub-rule (1), before the committee on such specified date and time the committee shall give specific recommendation in writing with respect to the request received from the Nodal Officer, based on the Information available with the committee.

(3) In case, such a person or intermediary, who has been served with the notice under sub-rule (1), is a foreign entity or body corporate as identified by the Designated Officer, notice shall be sent by way of letters or fax pr e-mail signed with electronic signatures to such foreign entity or body corporate and any such foreign entity or body corporate shall respond to such a notice within the time specified therein, failing which the committee shall given specific recommendation in writing with respect to the request received from the Nodal Officer, based on the information available with the committee.

(4) The committee referred to in rule 7 shall examine the request and printed sample information and consider whether the request is covered within the scope of sub-section (1) of section 69A of the Act and that it is justifiable to block such information or part thereof and shall give specific recommendation in writing with respect to the request received from the Nodal Officer.

(5) The Designated Officer shall submit the recommendation of the committee, in respect of the request for blocking of information alongwith the details sent by the Nodal Officer to the Secretary in the department of Information Technology under Ministry of Communication and Information Technology, Government of India (hereinafter referred to as the "Secretary, Department of Information Technology").

(6) The Designated Officer, on approval of the request by the Secretary, Department of Information Technology, shall direct any agency of the Giverment or the intermediary to block the offending information generated, transmitted, received, stored or hosted in their computer resource for public access within the time limit specified in the direction:

Provided that in case the request of the Nodal Officer is not approved by the Secretary, Department of Information Technology, the Designated Officer shall convey the same to such Nodal Officer.

### **9. Blocking of Information in cases of emergency.-**

(1) Notwithstanding anything contained in rules 7 and 8 the Designated Officer, in any case of emergency nature, for which no delay is acceptable, shall examine the request and printed sample information and consider whether the

request is within the scope of sub-section (1) of section 69A of the Act and it is necessary or expedient and justifiable to block such information or part thereof and submit the request with specified recommendation in writing to Secretary, Department of Information Technology.

(2) In case of emergency nature, the Secretary, Department of Information Technology may, if he satisfied that it is necessary or expedient and justifiable for blocking for public access of any information or part thereof through any computer resource and after recording reasons in writing, as an interim measure issue such directions as he may consider necessary to such identified or identifiable persons or intermediary in control of such computer resource hosting such information or part thereof without giving him an opportunity of hearing.

(3) The Designated Officer at the earliest but not later than forty-eight hours of issue of direction under sub-rule (2) shall bring the request before the committee referred to in rule 7 for its consideration and recommendation.

(4) On receipt of recommendations of committee, Secretary, Department of Information Technology, shall pass the final order as regard to approval of such request and in case the request for blocking its not approved by the Secretary, Department of Information Technology in his final order, the interim direction issued under sub-rule (2) shall be revoked and the person or intermediary in control of such information shall be accordingly directed to unblock the information for public access.

#### **10. Process of order of court for blocking of information.-**

In case of an order from a competent court in India for blocking of any information or part thereof generated transmitted, received, stored or hosted in a computer resource, the Designated Officer shall immediately on receipt of certified copy of the court order, submit it to the secretary, Department of Information Technology and initiate action as directed by the court.

#### **11. Expeditious disposal of request.-**

The request received from Nodal Officer shall be decided expeditiously which in no case shall be more than seven working days from the date of receipt of the request.

#### **12. Action for non-compliance of direction by intermediary.-**

In case the intermediary fails to comply with direction issued to him under rule 9, the Designated Officer shall, with the prior approval of the Secretary, Department of Information Technology, initiate appropriate action as may be required to comply with the provisions of sub-section (3) of section 69A of the Act.

#### **13. Intermediary to designate one person to receive and handle directions.-**

(1) Every intermediary shall designate at least one person to receive and handle the directions for blocking of access by the public any information generated transmitted, received, stored or hosted in any computer resource under these rules.

(2) The Designated person of the intermediary shall acknowledge receipt of the direction to the Designated Officer within two hours on receipt of the direction through acknowledgement letter or fax e-mail signed with electronic signature.

#### **14. Meeting of Review Committee.-**

The Review Committee shall meet at least once in two months and record its finding whether the directions issued under these rule are in accordance with the provisions of sub-section (1) of section 69A of the Act and it is of the opinion that the directions are not in accordance with the provisions referred to above, it may set aside the directions and issues order for unblocking of said information generated, transmitted, received, stored or hosted in any computer resource for public access.

#### **15. Maintenance of record by Designated Officer.-**

The Designated Officer shall maintain complete record of the request received and action taken thereof, in electronic database and also in register of the cases of blocking for public access of the information generated, transmitted, received, stored or hosted in any computer resource.

#### **16. Request and complaints to be confidential.-**

Strict confidentiality shall be maintained regarding all the request and complaints received and actions taken thereof.

### **FORM** **[See rule 6(2)]**

#### **A. Complaint**

1. Name of the complainant:- \_\_\_\_\_

(Person who has sent the complaint to the Ministry/Department/State Govt./Nodal Officer)

2. Address : \_\_\_\_\_

City \_\_\_\_\_ Pin Code: \_\_\_\_\_

3. Telephone : \_\_\_\_\_ (prefix STD code)

4. Fax (if any) : \_\_\_\_\_

5. Mobile (if any): \_\_\_\_\_

6. email (if any) : \_\_\_\_\_

**B. Detail of website /Computer resource / intermediary/ offending information hosted on the website**

(please give detail wherever known)

7. URL/ Web address: \_\_\_\_\_

8. IP Address: \_\_\_\_\_

9. Hyperlink: \_\_\_\_\_

10. Server/Proxy Server Address: \_\_\_\_\_

11. Name of the intermediary: \_\_\_\_\_

12. URL of the intermediary: \_\_\_\_\_

(please attach screenshot/printout of the offending information)

13. Address or location of intermediary in case the intermediary is telecom service provider, network service provider, internet service provider, web-hosting provider and cyber café or other form of intermediary for which information under points (7), (8), (8), (9), (10), (11) and (12) are not available.

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**C. Detail of Request for blocking**

14. Recommendation/Comment of the Ministry/State Govt.

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

15. The level at which the comment/recommendation have been approved  
(pleaser specify designation): \_\_\_\_\_

16. Have the complaint been examined in Ministry/State Government: Y/N

17. If yes, under which of the following reason it falls (please tick):

- (i) Interest of Sovereignty or integrity of India
- (ii) Defence of India
- (iii) Security of the State
- (iv) Friendly relations with foreign States
- (v) Public order
- (vi) for preventing intermediary to the commission of any cognizable offence relating to above.

**D. Detail of the Nodal Officer forwarding the complaint alongwith recommendation of the Ministry/State Govt. and related enclosures**

18. Name of the Nodal Officer: \_\_\_\_\_  
19. Designation: \_\_\_\_\_  
20. Organisation: \_\_\_\_\_  
21. Address: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
City: \_\_\_\_\_ Pin Code: \_\_\_\_\_  
22. Telephone: \_\_\_\_\_ (prefix STD Code)  
23. Fax (if any): \_\_\_\_\_  
24. Mobile (if any): \_\_\_\_\_  
25. email (if any): \_\_\_\_\_

**E. Any other information:**

**F. Enclosures:** 1.  
2.  
3.

Date:                      Place                                      Signature

**THE INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARD FOR MONITORING AND COLLECTING TRAFFIC DATA OR INFORMATION) RULES, 2009**

*In exercise of the powers conferred by clause (za) of sub-section (2) of section 87, read with sub-section (3) of section 69-B of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:-*

**1. Short title and commencement.-**

- (1) These rules may be called THE INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARD FOR MONITORING AND COLLECTING TRAFFIC DATA OF INFORMATION) Rules, 2009.
- (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 requires,-

- (a) “Act” means the Information Technology Act, 2000 (21 of 2000);
- (b) “Communication” means dissemination, transmission, carriage of information or signal in some manner and include both a direct communication and an indirect communication;

- (c) “Communication Link” means the use of satellite, microwave, radio, terrestrial line, wire, wireless or any other communication media to interconnect computer resources;
- (d) “Competent authority” means the Secretary to the Government of India in the Department of Information Technology under the Ministry of Communication and Information Technology;
- (e) “Computer resource” means computer resources as defined in clause(k) of sub-section (1) of section 2 of the Act;
- (f) “Cyber security incident” means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service/disruption, unauthorised use of a computer resources for processing or storage of information or changes to data, information without authorisation;
- (g) “Cyber security breaches” means unauthorised acquisition or unauthorised use by a person of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resources;
- (h) “Information” means information as defined in clause (v) of sub-section (1) of section 2 of the Act;
- (i) “Information security practices” means implementation of security policies and standards in order to minimize the cyber security incidents and breaches;
- (j) “Intermediary” means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;
- (k) “monitor” with its grammatical variation and cognate expressions, includes to view or inspect or record or collect traffic data or information generated, transmitted, received or stored in a computer resources by means of a monitoring device;
- (l) “Monitoring device” means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself in combination with any other instrument, device, equipment or apparatus, to view or inspect or record or collect traffic data or information;
- (m) “Port” or “application port” means a set of software rules which identifies and permits communication between application to application, network to network, computer to computer, computer system to computer system;
- (n) “Review Committee” means the Review Committee constituted under rule 419-A of the Indian Telegraphy Rules, 1951;
- (o) “security policy” means documented business rules and processes for protecting information and the computer resources;
- (p) “Traffic data” means traffic data as defined in Explanation (ii) to section 698 of the Act.

### 3. Direction for monitoring.-

(1) No directions for monitoring and collection of traffic data or information under sub-section (3) of section 69-B of the Act shall be issued, except by an order made by the competent authority.

(2) The Competent of authority may issue directions for monitoring for any or all of the following purpose related to cyber security, namely:-

- (a) Forecasting of imminent cyber incidents;
- (b) Monitoring network application with traffic data or information on computer resources;
- (c) Identification and determining of viruses or computer contaminant;
- (d) Tracking cyber security breaches or cyber security incidents;
- (e) Tracking computer resources breaching cyber security or spreading virus or computer contaminants;
- (f) Identifying or tracking of any person who has breached, or is suspected of having breached or being likely to breach cyber security;
- (g) Undertaking forensic of the concerned computer resources as a part of investigation or internal audit of information security practices in the computer resources.
- (h) Accessing a stored information for enforcement of any provisions of the laws relating to cyber security for the time being in force;
- (i) Any other matter relating to cyber security.

(3) Any direction issued by the competent authority under sub-rule (2) shall contain reasons for such direction and a copy of such direction shall be forwarded to the Review Committee within a period of seven working days.

(4) The direction of the competent authority for monitoring and collection of traffic data or information may include the monitoring and collecting of traffic data or information from any person or class of persons or relating to any particular subject whether such traffic data or information, or class of traffic data or information, are received with

one or more computer resources, being a computer resource likely to be used for the generation, transmission, receiving, storing of traffic data or information from or to one particular person or one or many set of premises.

#### **4. Authorised agency of Government for monitoring and collection of traffic data or information.-**

(1) The competent authority may authorise any agency of the Government for monitoring and collection of traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The agency authorised by the competent authority under sub-rule (1) shall designate one or more nodal officer, not below the rank of the Deputy Secretary to the Government of India, for the purpose to authenticate and send the requisition conveying direction issued under rule 3 to the designated officers of the concerned intermediary or person in-charge of computer resources.

(3) The requisition under sub-rule (2) shall specify the name and designation of the officer or the agency to whom the monitored or collected traffic data or information is to be disclosed.

(4) The intermediaries or person in-charge of computer resource shall designate one or more officers to receive requisition and to handle such requisition from the nodal officer for monitoring or collection of traffic data or information.

(5) The requisition conveying directions for monitoring shall be conveyed to the designated officers of the intermediary or person in-charge of computer resources, in writing through letter or fax by the nodal officer or delivered, (including delivery by e-mail signed with electronic signature), by an officer not below the rank of Under Secretary or officer of the equivalent rank.

(6) The nodal officer issuing the requisition conveying direction for monitoring under sub-rule (2) shall also make a request in writing to the designated officer of intermediary or person in-charge of computer resources for monitoring in accordance with the format indicated in such requisition and report the same to the officer designated under sub-rule(3).

(7) The nodal officer shall also make a request to the officer of intermediary or person in-charge of computer resource designated under sub-rule (4) to extend all facilities, co-operation and assistance in installation, removal and testing equipment and also enable online access or to secure and provide online access to the computer resource for monitoring and collecting traffic data or information.

(8) On receipt of requisition under sub-rule (2) conveying the direction issued under sub-rule (2) of rule 3, the designated officer of the intermediary or person in-charge of computer resource designated under sub-rule (4) shall acknowledge the receipt of requisition by way of letter or fax or electronically signed e-mail to the nodal officer within a period of two hours from the time of receipt of such requisition.

(9) The officer of the intermediary or person in-charge of computer resource designated under sub-rule (4) shall maintain proper records of the requisitions received by him.

(10) The designated officer of the intermediary or person in-charge of computer resource shall forward in every fifteen days a list of requisition conveying direction for monitoring or collection of traffic data or information to the nodal officer which shall include details such as the reference and date of requisition conveying direction of the concerned competent authority.

#### **5. Intermediary to ensure effective check in handling monitoring or collection of traffic data or information.-**

The intermediary or person in-charge of computer resources shall put in place adequate and effective internal checks to ensure that unauthorised monitoring or collection of traffic data or information does not take place and extreme secrecy is maintained and utmost care and precaution is taken in the matter of monitoring or collection of traffic data or information as it affects privacy of citizens and also that this matter is handled only by the designated officer of the intermediary or person in-charge of computer resource.

#### **6. Responsibility of intermediary.-**

The intermediary or person in-charge of computer resource shall be responsible for the actions of their employees also, and in case of violation of the provision of the Act and rules made there under pertaining to maintenance of secrecy and confidentiality of Information or any unauthorised monitoring or collection of traffic data or information, the intermediary or person in-charge of computer resource shall be liable for any action under the relevant provision of the laws for the time being in force.

#### **7. Review of directions of competent authority.-**

The review Committee shall meet at least once in two months and record its finding whether the directions issued under sub-rule (2) of rule 3 are in accordance with the provision of sub-section (3) of section 69-B of the Act and where the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above,

it may set aside the directions and issue order for destruction of the copies, including corresponding electronic record of the monitored or collected traffic data or information.

### **8. Destruction of records.-**

(1) Every record, including electronic records pertaining to such directions for monitoring or collection of traffic data shall be destroyed by the designated officer after the expiry of a period of nine months from the receipt of direction or creation of record, whichever is later, except in a case where the traffic data or information is, or likely to be, required for functional requirements.

(2) Save as otherwise required for the purpose of any ongoing investigation, criminal complaint or legal proceedings the intermediary or the person in-charge of computer resource shall destroyed records pertaining to directions for monitoring or collection of information within a period of six months of discontinuance of the monitoring or collection of traffic data and in doing so they shall maintain extreme secrecy.

### **9. Prohibition of monitoring or collection of traffic data or information without authorisation.-**

(1) Any person who, intentionally or knowingly, without authorisation under sub-rule (2) of rule 3 or sub-rule (1) of rule 4, monitors or collects traffic data or information, or attempts to monitor or collect traffic data or information, or authorise s or assists any person to monitor or collect traffic data or information in the course of its occurrence or transmission at any place within India, shall be proceeded against, punished accordingly under the relevant provisions of the law for the time being in force.

(2) The monitoring or collection of traffic data or information in computer resources by the employees of an intermediary or person in-charge of computer resource or a person duly authorised by the intermediary, may be undertaken in course of his duty relating to the services provided by that intermediary, if such activities are reasonably necessary for the discharge his duties as per the prevailing industry practices, in connection with the following matters, namely:-

- (i) Installation of computer resource or any equipment to be used with computer resource; or
- (ii) Operation or maintenance of computer resource; or
- (iii) Installation of any communication link or software either at the end of the intermediary or subscriber, or installation of user account on the computer resource of intermediary and testing of the same for its functionality;
- (iv) Accessing stored information from computer resource relating to the installation, connection or maintenance of equipment, computer resource or a communication link or code; or
- (v) Accessing stored information from computer resource for the purpose of-
  - (a) Implementing information security practices in the computer resources;
  - (b) Determining any security breaches, computer contaminant or computer virus;
  - (c) Undertaking forensics of the concerned computer resource as a part of investigation or internal audit; or
- (vi) Accessing or analyzing information from a computer resource for the purpose of tracing a computer resource or any person who has contravened, any provision of the Act this is likely to have an adverse impact on the services provided by the intermediary.

(3) The intermediary or the person in-charge of computer resource and its employees shall maintain strict secrecy and confidentiality of information while performing the actions as specified under sub-rule (2).

(4) The details of monitored or collected traffic data or information shall not be used or disclosed by intermediary or person in-charge of computer resource or any of its employees to any person other than the intended recipient of the said information under sub-rule (2) of rule 4. Any intermediary or its employees or person in-charge of computer resource who contravenes the provision of this rule shall be proceeded against and punished accordingly under the relevant provisions of the Act or any other law for the time being in force.

### **10. Prohibition of disclosure of traffic data or information by authorised agency.-**

The details of monitored or collected traffic data or information shall not be used or disclosed by the agency authorless under sub-rule (1) of rule 4 for any other purpose, except for forecasting imminent cyber threats or general trend of port-wise traffic on Internet, or general analysis of cyber incidents, or for investigation or in judicial proceedings before the competent Court in India.

### **11. Maintenance of confidentiality.-**

Save as otherwise provided in rule 10, strict confidentiality shall be maintained in respect of directions for monitoring or collection of traffic data or information issued by the competent authority under these rules.

## THE INFORMATION TECHNOLOGY (ELECTRONIC SERVICE DELIVERY) RULES, 2011

*G.S.R. (E) - In exercise of the powers conferred by clause (ca) of sub-section (2) of section 87, read with sub-section (2) of section 6A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:*

### 1. Short title and commencement.-

- (1) These rules may be called the Information Technology (Electronic Service Delivery) Rules, 2011.
- (2) They shall come into force on the date of their publication in the Official Gazette.

### 1. Definitions.-

In these rules, unless the context otherwise requires,

- a) **"Act"** means the Information Technology Act, 2000 (21 of 2000);
- b) **"Appropriate Government"** means the Central Government or the State Government or an Union Territory Administration;
- c) **"Authorised agent"** means an agent of the appropriate Government or service provider and includes an operator of an electronically enabled kiosk who is permitted under these rules to deliver public services to the users with the help of a computer resource or any communication device, by following the procedure specified in the rules;
- d) **"certificate"** means a certificate required to be issued by a statutory authority empowered under any Act, rule, regulation or Order of the appropriate Government to issue a certificate to confirm the status, right or responsibility of a person, either natural or artificial, and includes a certificate in electronic form printed and delivered in such form as may be specified by the appropriate authority;
- e) **"Certifying Authority"** means certifying authority as defined in clause (g) of sub-section (1) of section 2 of the Act;
- f) **"communication device"** means the communication device as defined in clause (ha) of sub-section (1) of section 2 of the Act;
- g) **"computer resource"** means the computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;
- h) **"Electronically enabled kiosk"** means the cyber café as defined in clause (na) of sub-section (1) of section 2 of the Act;
- i) **"Electronic Service Delivery"** means the delivery of public services in the form of filing receipt of forms and applications, issue or grant of any license, permit, certificate, sanction or approval and the receipt or payment of money by electronic means by following the procedure specified under rule 3;
- j) **"Electronic signature"** means the electronic signature as defined in clause (ta) of sub-section (1) of section 2 of the Act;
- k) **"Electronic Signature Certificate"** means the electronic signature certificate as defined in clause (tb) of sub-section (1) of section 2 of the Act;
- l) **"Repository of Electronically Signed Electronic Records"** means a collection of all electronically signed electronic records, stored and managed in accordance with these rules;
- m) **"service provider"** means a service provider as referred to in Explanation to sub-section (1) of section 6A of the Act;
- n) **"signing authority "** means an authority empowered under any Act, rules, regulations or Order of the appropriate Government to issue a certificate.

### 3. System of Electronic Service Delivery.

(1) The appropriate Government may on its own or through an agency authorised by it, deliver public services through electronically enabled kiosks or any other electronic service delivery mechanism.

(2) The appropriate Government or its agencies may specify the form and the manner of Electronic Service Delivery.

(3) The appropriate Government may determine the manner of encrypting sensitive electronic records requiring confidentiality, while they are electronically signed.

(4) The appropriate Government shall notify the service providers and their agents authorised for Electronic Service

Delivery.

(5) The appropriate Government may allow receipt of payments made by adopting the Electronic Service Delivery System to be a deemed receipt of payment effected in compliance with the financial code and treasury code of such Government.

(6) The appropriate Government may authorise service providers or their authorised agents to collect, retain and appropriate such service charges as may be specified by the appropriate Government for the purpose of providing such services from the person availing such services:

Provided that the apportioned service charges shall be clearly indicated on the receipt to be given to the person availing the services.

(7) The appropriate Government shall by notification specify the scale of service charges which may be charged and collected by the service providers and their authorised agents for various kinds of services.

(8) The appropriate Government may also determine the norms on service levels to be complied with by the Service Provider and the authorised agents.

#### **4. Notification of Electronic Service Delivery.-**

(1) The appropriate Government may notify the services that shall be delivered electronically from time to time.

(2) The appropriate Government may identify and notify, from time to time, the list or signing authorities in respect of different classes of licenses, permits, certificates, sanctions, payment receipt approvals and local limits of their respective jurisdictions.

(3) The notification shall specify the nature of certificate, the names of the signing authorities, as approved by the appropriate Government, the period of effectiveness of the authority and the extent of their jurisdiction.

(4) The appropriate Government may notify changes to the list of signing authorities from time to time, taking into consideration the terms and conditions of the services of employees holding positions of signing authorities.

#### **5. Creation of repository of electronically signed electronic records by Government Authorities.**

(1) All authorities that issue any license, permit, certificate, sanction or approval electronically, shall create, archive and maintain a repository of electronically signed electronic records of such licenses, permits, certificates, sanctions or approvals, as the case may be, online with due timestamps of creation of these individual electronic records.

(2) The appropriate Government may specify the manner of creating, establishing, archiving and maintaining the repository of electronically signed electronic records referred to in sub-rule (1).

(3) The authorities may electronically sign the electronic records of such licenses, permits, certificates, sanctions or approvals for each record or as a whole for a specific duration and shall be responsible in administering them online.

(4) The appropriate Government may specify the security procedures in respect of the electronic data, information, applications, repository of digitally signed electronic records and information technology assets under their respective control and that security procedures shall be followed by the Head of the Department and the signing authorities.

**Explanation.-** The expression “security procedures” referred to in sub-rule (4) shall include requirements for the storage and management of cryptographic keys, restrictions for downloading the certificates on to browsers, and of complying with the requirements of certifying authorities.

#### **6. Procedure for making changes in a repository of electronically signed electronic records.-**

(1) The appropriate Government may either suo moto or after receiving an application from an interested party, make or order to make an appropriate change in a repository of electronically signed electronic records along with recording the reasons for making such a change.

(2) Any change effected to any record in a repository of electronically signed electronic records and any addition or deletion of a record from such repository shall be electronically signed by the person who is authorised to make such changes along with the time stamps of original creation and modification times.

(3) The appropriate Government may determine the manner of electronically signing the event of deletion of a record from the repository of electronically signed electronic records.

(4) The appropriate Government may also determine the manner of provisioning secure access to the repository of digitally signed electronic records.

(5) The appropriate Government may also determine the requirements for maintaining audit trails of all changes made to repository of digitally signed electronic records.

### **7. Responsibility of service provider and authorised agents for financial management and accounting.-**

The appropriate Government may direct every service provider and authorised agent to keep an updated and accurate account of the transactions, receipts, vouchers and specify the formats for maintaining accounts of transactions and receipt of payment in respect of the electronic services delivered and the said records shall be produced for inspection and audit before an agency or person nominated by the appropriate Government.

### **8. Audit of the Information System and Accounts of service provider and authorised agents.**

(1) The appropriate Government may cause an audit to be conducted of the affairs of the service providers and authorised agents in the State at such intervals as deemed necessary by nominating such audit agencies.

(2) The audit may cover aspects such as the security, confidentiality and the privacy of information, the functionality and performance of any software application used in the electronic service delivery and the accuracy of accounts kept by the service providers and authorised agents.

(3) The service providers and the authorised agents shall provide such information and assistance to the audit agencies nominated by the appropriate authority, to comply with the directions given by the audit agencies and to rectify the defects and deficiencies pointed out by the audit agencies within the time limit specified by the audit agency.

(4) All serviceproviders and the authorised agents shall submit a due declaration for protecting the data of every individual transaction and citizen and any unauthorised disclosure to anyone without the written consent of either the individual or the appropriate Government shall be debarred from providing such a service any further and the provisions of section 45 of the Act shall be applicable in such cases.

### **9. Use of special stationery in electronic service delivery.-**

The appropriate Government may specify different types of special stationery, with accompanying security features for forms, applications, licenses, permits, certificates, receipts of payment and such other documents as part of Electronic Service Delivery.

## **THE INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011**

*G.S.R (E).— In exercise of the powers conferred by clause (ob) of subsection (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely.—*

### **1. Short title and commencement.—**

(1) These rules may be called the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

(2) They shall come into force on the date of their publication in the Official Gazette.

### **2. Definitions.—**

(1) In these rules, unless the context otherwise requires,-

- (a) “Act” means the Information Technology Act, 2000 (21 of 2000);
- (b) “Biometrics” means the technologies that measure and analyse human body characteristics, such as ‘fingerprints’, ‘eye retinas and irises’, ‘voice patterns’, ‘facial patterns’, ‘hand measurements’ and ‘DNA’ for authentication purposes;
- (c) “Body corporate” means the body corporate as defined in clause (i) of explanation to section 43A of the Act;
- (d) “Cyber incidents” means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;
- (e) “Data” means data as defined in clause (o) of sub-section (1) of section 2 of the Act;
- (f) “Information” means information as defined in clause (v) of sub-section (1) of section 2 of the Act;
- (g) “Intermediary” means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;

- (h) “Password” means a secret word or phrase or code or pass phrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information;
- (i) “Personal information” means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

### **3. Sensitive personal data or information.—**

Sensitive personal data or information of a person means such personal information which consists of information relating to;—

- (i) password;
- (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
- (iii) physical, physiological and mental health condition;
- (iv) sexual orientation;
- (v) medical records and history;
- (vi) Biometric information;
- (vii) any detail relating to the above clauses as provided to body corporate for providing service; and
- (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

### **4. Body corporate to provide policy for privacy and disclosure of information.—**

(1) The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. Such policy shall be published on website of body corporate or any person on its behalf and shall provide for—

- (i) clear and easily accessible statements of its practices and policies;
- (ii) type of personal or sensitive personal data or information collected under rule 3;
- (iii) purpose of collection and usage of such information;
- (iv) disclosure of information including sensitive personal data or information as provided in rule 6;
- (v) reasonable security practices and procedures as provided under rule 8.

### **5. Collection of information.—**

(1) Body corporate or any person on its behalf shall obtain consent in writing through letter or fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

- (2) Body corporate or any person on its behalf shall not collect sensitive personal data or information unless —
  - (a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and
  - (b) the collection of the sensitive personal data or information is considered necessary for that purpose.

(3) While collecting information directly from the person concerned, the body corporate or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of —

- (a) the fact that the information is being collected;
- (b) the purpose for which the information is being collected;
- (c) the intended recipients of the information; and
- (d) the name and address of —
  - (i) the agency that is collecting the information; and
  - (ii) the agency that will retain the information.

(4) Body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force..

(5) The information collected shall be used for the purpose for which it has been collected.

(6) Body corporate or any person on its behalf shall permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible:

Provided that a body corporate shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by the provider of information to such body corporate or any other person acting on behalf of such body corporate.

(7) Body corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or

Otherwise, also have an option to withdraw its consent given earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought.

(8) Body corporate or any person on its behalf shall keep the information secure as provided in rule 8.

(9) Body corporate shall address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. For this purpose, the body corporate shall designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer shall redress the grievances of provider of information expeditiously but within one month from the date of receipt of grievance.

## **6. Disclosure of information.—**

(1) Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation:

Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

(2) Notwithstanding anything contained in sub-rule (1), any sensitive personal data or Information shall be disclosed to any third party by an order under the law for the time being in force.

(3) The body corporate or any person on its behalf shall not publish the sensitive personal data or information.

(4) The third party receiving the sensitive personal data or information from body corporate or any person on its behalf under sub-rule (1) shall not disclose it further.

## **Transfer of information.-**

A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

## **Reasonable Security Practices and Procedures.—**

(1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

(2) The International Standard IS/ISO/IEC 27001 on “Information Technology – Security Techniques – Information Security Management System – Requirements” is one such standard referred to in sub-rule (1).

(3) Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

(4) The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant up gradation of its process and computer resource.

## **THE INFORMATION TECHNOLOGY (INTERMEDIARIES GUIDELINES) RULES, 2011**

*G.S.R (E).— In exercise of the powers conferred by clause (zg) of subsection (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely: —*

### **1. Short title and commencement.—**

- (1) These rules may be called the Information Technology (Intermediaries guidelines) Rules, 2011.
- (2) They shall come into force on the date of their publication in the Official Gazette.

### **2. Definitions.—**

- (1) In these rules, unless the context otherwise requires,—
  - (a) “Act” means the Information Technology Act, 2000 (21 of 2000);
  - (b) “Communication link” means a connection between a hypertext or graphical element (button, drawing, image) and one or more such items in the same or different electronic document wherein upon clicking on a hyperlinked item, the user is automatically transferred to the other end of the hyperlink which could be another document or another website or graphical element.
  - (c) “Computer resource” means computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;
  - (d) “Cyber security incident” means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;
  - (e) “Data” means data as defined in clause (o) of sub-section (1) of section 2 of the Act;
  - (f) "Electronic Signature" means electronic signature as defined in clause (ta) of sub-section (1) of section 2 of the Act;
  - (g) “Indian Computer Emergency Response Team” means the Indian Computer Emergency Response Team appointed under sub section (1) of section 70(B) of the Act;
  - (h) “Information” means information as defined in clause (v) of sub-section (1) of section 2 of the Act;

- (i) “Intermediary” means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;
- (j) “User” means any person who access or avail any computer resource of intermediary for the purpose of hosting, publishing, sharing, transacting, displaying or uploading information or views and includes other persons jointly participating in using the computer resource of an intermediary.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

### **3. Due diligence to be observed by intermediary.—**

The intermediary shall observe following due diligence while discharging his duties, namely : —

(1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary’s computer resource by any person.

(2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —

- (a) belongs to another person and to which the user does not have any right to;
- (b) is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, pedophilic, libelous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;
- (c) harm minors in any way;
- (d) infringes any patent, trademark, copyright or other proprietary rights;
- (e) violates any law for the time being in force;
- (f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;
- (g) impersonate another person;
- (h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;
- (i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation.

(3) The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2):

Provided that the following actions by an intermediary shall not amount to hosting, publishing, editing or storing of any such information as specified in sub-rule (2) —

- (a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource;
- (b) removal of access to any information, data or communication link by an intermediary after such information, data or communication link comes to the actual knowledge of a person authorised by the intermediary pursuant to any order or direction as per the provisions of the Act;

(4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes.

(5) The Intermediary shall inform its users that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the Intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove non-compliant information..

(6) The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.

(7) When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.

(8) The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable security practices and procedures and sensitive personal information) Rules, 2011.

(9) The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.

(10) The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force:

Provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.

(11) The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule 3 can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint.

## **THE INFORMATION TECHNOLOGY (GUIDELINES FOR CYBER CAFE) RULES, 2011**

G.S.R. (E).— In exercise of the powers conferred by clause (zg) of subsection (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:—

### **1. Short title and commencement.—**

- (1) These rules may be called the Information Technology (Guidelines for Cyber Cafe) Rules, 2011.
- (2) They shall come into force on the date of their publication in the Official Gazette.

### **2. Definitions.—**

- (1) In these rules, unless the context otherwise requires,-
  - (a) “Act” means the Information Technology Act, 2000 (21 of 2000);
  - (b) “Appropriate Government” means the Central Government or the State Government or an Union Territory Administration;
  - (c) “Cyber Cafe” means cyber café as defined in clause (na) of sub-section (1) of section 2 of the Act;
  - (d) “computer resource” means a computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;
  - (e) “Data” means data as defined in clause (o) of sub-section (1) of section 2 of the Act;
  - (f) “Information” means information as defined in clause (v) of sub-section (1) of section 2 of the Act;
  - (g) “Intermediary” means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;
    - (aa) “Registration Agency” means an agency designated by the Appropriate Government to register cyber café for their operation;
    - (bb) “Log Register” – means a register maintained by the Cyber Café for access and use of computer resource;
    - (cc) “User” means a person who avails or access the computer resource and includes other persons jointly participating in availing or accessing the computer resource in a cyber café.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

### **3. Agency for registration of cyber café.—**

- (1) All cyber cafes shall be registered with a unique registration number with an agency called as registration

agency as notified by the Appropriate Government in this regard. The broad terms of registration shall include:

- a. name of establishment;
- b. address with contact details including email address;
- c. whether individual or partnership or sole proprietorship or society or company;
- d. date of incorporation;
- e. name of owner/partner/properiter/director;
- f. whether registered or not (if yes, copy of registration with Registrar of Firms or Registrar of Companies or Societies); and
- g. type of service to be provided from cyber café

Registration of cyber café may be followed up with a physical visit by an officer from the registration agency.

(2) The details of registration of cyber café shall be published on the website of the registration agency.

(3) The Appropriate Government shall make an endeavour to set up on-line registration facility to enable cyber café to register on-line.

(4) The detailed process of registration to be mandatorily followed by each Registration Agency notified by the Appropriate Government shall be separately notified under these rules by the central Government.

#### **4. Identification of User.—**

(1) The Cyber Café shall not allow any user to use its computer resource without the identity of the user being established. The intending user may establish his identity by producing a document which shall identify the users to the satisfaction of the Cyber Café. Such document may include any of the following :—

- (i) Identity card issued by any School or College; or
- (ii) Photo Credit Card or debit card issued by a Bank or Post Office; or
- (iii) Passport; or
- (iv) Voter Identity Card; or

(2) The Cyber Café shall keep a record of the user identification document by either storing a photocopy or a scanned copy of the document duly authenticated by the user and authorised representative of cyber café. Such record shall be securely maintained for a period of at least one year.

(3) In addition to the identity established by an user under sub-rule (1), he may be photographed by the Cyber Café using a web camera installed on one of the computers in the Cyber Café for establishing the identity of the user. Such web camera photographs, duly authenticated by the user and authorised representative of cyber café, shall be part of the log register which may be maintained in physical or electronic form.

(4) A minor without photo Identity card shall be accompanied by an adult with any of the documents as required under sub-rule (1).

(5) A person accompanying a user shall be allowed to enter cyber café after he has established his identity by producing a document listed in sub-rule (1) and record of same shall be kept in accordance with sub-rule (2).

(6) The Cyber café shall immediately report to the concerned police, if they have reasonable doubt or suspicion regarding any user.

#### **5. Log Register.—**

(1) After the identity of the user and any person accompanied with him has been established as per sub-rule (1) of rule 4, the Cyber Café shall record and maintain the required information of each user as well as accompanying person, if any, in the log register for a minimum period of one year.

(2) The Cyber Café may maintain an online version of the log register. Such online version of log register shall be authenticated by using digital or electronic signature. The log register shall contain at least the following details of the user, namely :—

- i. Name
- ii. Address
- iii. Gender
- iv. Contact Number
- v. Type and detail of identification document
- vi. Date
- vii. Computer terminal identification
- viii. Log in Time
- ix. Log out Time

(3) Cyber Café shall prepare a monthly report of the log register showing date-wise details on the usage of the

computer resource and submit a hard and soft copy of the same to the person or agency as directed by the registration agency by the 5th day of next month.

(4) The cyber café owner shall be responsible for storing and maintaining backups of following log records for each access or login by any user of its computer resource for at least one year:—

- (i) History of websites accessed using computer resource at cyber café;
- (ii) Logs of proxy server installed at cyber café.

Cyber Café may refer to “Guidelines for auditing and logging – CISG-2008-01” prepared and updated from time to time by Indian Computer Emergency Response Team (CERT-In) for any assistance related to logs. This document is available at [www.cert-in.org.in](http://www.cert-in.org.in)

(5) Cyber café shall ensure that log register is not altered and maintained in a secure manner for a period of at least one year.

## **6. Management of Physical Layout and computer resource.—**

(1) Partitions of Cubicles built or installed if any, inside the Cyber Café, shall not exceed four and half feet in height from the floor level.

(2) The screen of all computers, installed other than in Partitions or Cubicles, shall face ‘outward’, i.e. they shall face the common open space of the Cyber Café.

(3) Any Cyber Café having cubicles or partitions shall not allow minors to use any computer resource in cubicles or partitions except when they are accompanied by their guardians or parents.

(4) All time clocks of the computer systems and servers installed in the Cyber Café shall be synchronised with the Indian Standard Time.

(5) All the computers in the cyber café may be equipped with the commercially available safety or filtering software so as to the avoid, as far as possible, access to the websites relating to pornography including child pornography or obscene information..

(6) Cyber Café shall take sufficient precautions to ensure that their computer resource are not utilised for any illegal activity.

(7) Cyber Café shall display a board, clearly visible to the users, prohibiting them from viewing pornographic sites as well as copying or downloading information which is prohibited under the law.

(8) Cyber Café shall incorporate reasonable preventive measures to disallow the user from tampering with the computer system settings.

(9) Cyber café shall maintain the user identity information and the log register in a secure manner.

(10) Cyber café shall also maintain a record of its staff for a period of one year.

(11) Cyber café shall not misuse or alter the information in the log register.

## **7. Inspection of Cyber Café -**

(1) An officer authorised by the registration agency, is authorised to check or inspect cyber café and the computer resource or network established therein at any time for the compliance of these rules. The cyber café owner shall provide every related document, registers and any necessary information to the inspecting officer on demand.