

[To be published in THE GAZETTE OF INDIA, EXTRAORDINARY, Part II, Section 3, Sub-section (i) of dated the 11th April 2011]

Government of India
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(Department of Information Technology)

NOTIFICATION

New Delhi, the -----, 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.

2. 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 cafe 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 service providers 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.

[No 11(3)/2011-CLFE]

(Shankar Aggarwal)
Additional Secretary to the Government of India

[To be published in THE GAZETTE OF INDIA, EXTRAORDINARY, Part II, Section 3, Sub-section (i) of dated the 11th April 2011]

Government of India
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(Department of Information Technology)

NOTIFICATION

New Delhi, the -----, 2011

G.S.R (E).— In exercise of the powers conferred by clause (ob) of sub-section (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 passphrase 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.

7. 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.

8. 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 upgradation of its process and computer resource.

No. 11(3)/2011-CLFE

(N. Ravi Shanker)

Joint Secretary to the Government of India

[To be published in THE GAZETTE OF INDIA, EXTRAORDINARY, Part II, Section 3, Sub-section (i) of dated the 11th April 2011]

Government of India
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(Department of Information Technology)

NOTIFICATION

New Delhi, the -----, 2011

G.S.R (E).— In exercise of the powers conferred by clause (zg) of sub-section (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,—

- (j) "Act" means the Information Technology Act, 2000 (21 of 2000);
- (k) "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.
- (l) "Computer resource" means computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;
- (m) "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;
- (n) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;
- (o) "Electronic Signature" means electronic signature as defined in clause (ta) of sub-section (1) of section 2 of the Act;

- (p) "Indian Computer Emergency Response Team" means the Indian Computer Emergency Response Team appointed under sub section (1) of section 70(B) of the Act;
 - (q) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;
 - (r) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;
 - (s) "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, paedophilic, libellous, 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.

[No. 11(3)/2011-CLFE]

(N. Ravi Shanker)
Joint Secretary to the Government of India

[To be published in THE GAZETTE OF INDIA, EXTRAORDINARY, Part II, Section 3, Sub-section (i) of dated the 11th April 2011]

Government of India
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(Department of Information Technology)

NOTIFICATION

New Delhi, the -----, 2011

G.S.R. (E).— In exercise of the powers conferred by clause (zg) of sub-section (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,—

- (t) “Act” means the Information Technology Act, 2000 (21 of 2000);
- (u) “Appropriate Government” means the Central Government or the State Government or an Union Territory Administration;
- (v) “Cyber Cafe” means cyber café as defined in clause (na) of sub-section (1) of section 2 of the Act;
- (w) “computer resource” means a computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;
- (x) “Data” means data as defined in clause (o) of sub-section (1) of section 2 of the Act;
- (y) “Information” means information as defined in clause (v) of sub-section (1) of section 2 of the Act;
- (z) “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/proprietor/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
- (v) Permanent Account Number (PAN) card issued by Income-Tax Authority; or

(vi) Photo Identity Card issued by the employer or any Government Agency;
or

(vi) Driving License issued by the Appropriate Government; or

(vii) Unique Identification (UID) Number issued by the Unique Identification Authority of India (UIDAI).

(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 cafe. 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

(vii) 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

(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 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.

[No. 11(3)/2011-CLFE]

(N. Ravi Shanker)
Joint Secretary to the Government of India