NOTIFICATION

New Delhi, the 11th April, 2011

G.S.R. 314(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 hyperlink 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 website or graphical element.

(c) "Computer resource" means computer resources as defined in clause (k) of sub-section (1) of section 2 of the Act;

(d) "Cyber security incidnt" means any real or suspected adverse event in relation to cyber security that violates an explicity or implicity applicable security policy resulting in unauthotrised 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) 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) Ail 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 he 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 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 hosing, 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 lights 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 staling 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.

[F. No. 11(3)/2011-CLFE]
N. RAVI SHANKER, Jt. Secy.

NOTIFICATION

New Delhi, the 11th April, 2011

G.S.R. 315(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,--

(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 cafe 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;

(h) "Registration Agency" means an agency designated by the Appropriate Government to register cyber cafe for their operation;

(i) "Log Register" - means a register maintained by the Cyber Cafe for access and use of computer resource;

(j) "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 cafe.

(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 cafe.— (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:

(i) name of establishment;
(ii) address with contact details including email address;
(iii) whether individual or partnership or sole properitership or society or company;
(iv) date of incorporation;
(v) name of owner/partner/properiter/director;
(vi) whether registered or not (if yes, copy of registration with Registrar of Firms or Registrar of Companies or Societies); and
(vii) type of service to be provided from cyber cafe

Registration of cyber cafe may be followed up with a physical visit by an officer from the registration agency.

(2) The details of registration of cyber cafe 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 cafe 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 Cafe shall not allow any user to use its computer resource without the identity of the user being established. The intending user may establish his identify by producing a document which shall identify the users to the satisfaction of the Cyber Cafe. 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 Cafe 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 Cafe using a web camera installed on one of the computers in the Cyber Cafe for establishing the identity of the user. Such web camera photographs, duly authenticated by the user and authorised representative of cyber cafe, 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 cafe 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 cafe 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 Cafe 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 Cafe 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 : —

(ii) Name
(iii) Address
(iv) Gender
(v) Contact Number
(vi) Type and detail of identification document
(vii) Date
(vii) Computer terminal identification
(viii) Log in Time
(ix) Log out Time

(3) Cyber Cafe 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 cafe 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 atleast one year:—

(i) History of websites accessed using computer resource al cyber cafe;
(ii) Logs of proxy server installed at cyber cafe.

Cyber Cafe 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-ln) for any assistance related to logs. This document is available at www.cert-in.org.in

(5) Cyber cafe 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 Cafe, 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 Cafe.

(3) Any Cyber Cafe 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 Cafe shall be synchronised with the Indian Standard Time.

(5) All the computers in the cyber cafe 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 Cafe shall take sufficient precautions to ensure that their computer resource are not utilised for any illegal activity.

(7) Cyber Cafe 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 Cafe shall incorporate reasonable preventive measures to disallow the user from tampering with the computer system settings.

(9) Cyber cafe shall maintain the user identity information and the log register in a secure manner.

(10) Cyber cafe shall also maintain a record of its stafr for a period of one year

(11) Cyber cafe shall not misuse or alter the information in the log register.

7. **Inspection of Cyber Cafe** : (1) An officer autnorised by the registration agency, is authorised to check or inspect cyber cafe and the computer resource of network established therein, at any time for the compliance of these rules. The cyber cafe owner shall provide every related document, registers and any necessary information to the inspecting officer on demand.

[F. No. 11(3)/2011-CLFE]
N. RAVI SHANKER, Jt. Secy.