[To be published in THE GAZETTE OF INDIA, EXTRAORDINARY, Part II, Section 3, Sub-section (i) of dated the ----------, 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 (Due diligence observed by intermediaries guidelines) 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) "Blog" means a type of website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video. Usually blog is a shared on-line journal where users can post diary entries about their personal experiences and hobbies;

(c) "Blogger" means a person who keeps and updates a blog;

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

(e) "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, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorisation;

(f) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;

(g) "Electronic Signature" means electronic signature as defined in clause (ta) of sub-section (1) of section 2 of the Act;

(h) "Indian Computer Emergency Response Team" means the Indian Computer Emergency Response Team appointed under sub section (1) of section 70(B) of the Act;

(i) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;

(j) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;

(k) "User" means any person including blogger who uses any computer resource for the purpose of sharing information, views or otherwise and includes other persons jointly participating in using the computer resource of intermediary.

3. Due Diligence observed by intermediary.— The intermediary shall observe following due diligence while discharging its duties.-

(1) The intermediary shall publish the terms and conditions of use of its website, user agreement, privacy policy etc..

(2) The intermediary shall notify users of computer resource not to use, display, upload, modify, publish, transmit, update, share or store any information that : —

(a) belongs to another person;

(b) is harmful, threatening, abusive, harassing, blasphemous, objectionable, defamatory, vulgar, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically or otherwise 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) discloses sensitive personal information of other person or to which the user does not have any right to;

(g) causes annoyance or inconvenience or deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;

(h) impersonate another person;

(i) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

(j) 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 itself host or publish or edit or store 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).

(4) The intermediary upon obtaining actual knowledge by itself or been brought to actual knowledge by an authority mandated under the law for the time being in force in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act expeditiously to work with user or owner of such information to remove access to such information that is claimed to be infringing or to be the subject of infringing activity. Further the intermediary shall inform the police about such information and preserve the records for 90 days.

(5) The Intermediary shall inform its users that in case of non-compliance with terms of use of the services and privacy policy provided by the Intermediary, the Intermediary has the right to immediately terminate the access rights of the users to the site of Intermediary.

(6) The intermediary shall follow provisions of the Act or any other laws for the time being in force.

(7) The intermediary shall not disclose sensitive personal information.

(8) Disclosure of information by intermediary to any third party shall require prior permission or consent from the provider of such information, who has provided such information under lawful contract or otherwise.

(9) Intermediary shall provide information to government agencies who are lawfully authorised for investigative, protective, cyber security or intelligence activity. The information 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 written request stating clearly the purpose of seeking such information.

(10) The information collected by the intermediary shall be used for the purpose for which it has been collected.

(11) The intermediary shall take all measures to secure its computer resource and integrity of information received, stored, transmitted or hosted shall be ensured.

(12) The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.

(13) The intermediary shall not deploy or install or modify the technological measures 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.

(14) The intermediary shall publish on its website the designated agent to receive notification of claimed infringements.