[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 (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 information) 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) "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 body corporate as defined in clause (i) of Explanation of section 43A of the Act;

(d) "Call data record" means a data record that contains information related to a telephone call, such as the origination and destination addresses of the call, the time the call started and ended, the duration of the call, the time of day the call was made and any toll charges that were added through the network or charges for operator services, among other details of the call;

(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 that one uses to gain admittance or access to information.

3. Sensitive personal data or information.— Sensitive personal data or information of a person shall include information collected, received, stored, transmitted or processed by body corporate or intermediary or any person, consisting of :

(i) password;

(ii) user details as provided at the time of registration or thereafter;

(iii) information related to financial information such as Bank account / credit card / debit card / other payment instrument details of the users;

(iv) Physiological and mental health condition;

(v) Medical records and history;

(vi) Biometric information;

(vii) Information received by body corporate for processing, stored or processed under lawful contract or otherwise;

(viii) Call data records;

Provided that, any information that is freely available or accessible in public domain or accessible 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 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 shall provide a privacy policy for handling of or dealing in user information including sensitive personal 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 provide for:

(i) Type of personal or sensitive information collected under sub-rule (ii) of rule 3;
(ii) Purpose, means and modes of usage of such information;
(iii) Disclosure of information as provided in rule 6.

5. Collection of information.— (1) Body corporate or any person on its behalf shall obtain consent of the provider of the information regarding purpose, means and modes of uses before collection of such information.

(2) Body corporate or any person on its behalf shall not collect sensitive personal information unless -

(a) the information is collected for a lawful purpose connected with a function or activity of the agency; and
(b) the collection of the information is necessary for that purpose.

(3) While collecting information directly from the individual concerned, the body corporate or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the individual concerned is aware of :

(a) the fact that the information is being collected; and
(b) the purpose for which the information is being collected; and
(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 hold the information.

(4) Body corporate or any person on its behalf holding sensitive personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

(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 users to review the information they had provided and modify the same, wherever necessary.

(7) Body corporate or any person on its behalf shall provide an option to the provider of the information to opt-in or opt-out.

(8) Body corporate or any person on its behalf shall keep the information secure.

(9) Body corporate shall address any discrepancies and grievances of their users with respect to processing of information in a time bound manner.

6. Disclosure of information.— (1) Disclosure of 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:

Provided that the information shall be provided to government agencies for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, and punishment of offences. The government agency shall send a written request to the body corporate possessing the sensitive information stating clearly the purpose of seeking such information. The government agency shall also state that the information thus obtained will not be published or shared with any other person.

(2) Without prejudice to sub-rule (1) of Rule 6, any 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 information.

(4) The third party receiving the information from body corporate as per sub-rule (1) shall not disclose it further.

7. Reasonable Security Practices and Procedures.— (1) Any person, including a body corporate shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards which shall require 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. In the event of an information security breach, any such person, including the body corporate 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" has been adopted by the country. The security practices prescribed by this standard are enshrined in the principle outlined in sub-rule (1).

(3) Industry associations or industry cluster who are following other than IS/ISO/IEC 27001 codes of best practices for data protection and fulfil the requirement of sub-rule (1), shall get their codes of best practices approved by the government, which shall be duly notified.

(4) The body corporate who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures.