# The Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009

**Notification, New Delhi, the 27th October, 2009, G.S.R. 782 (E).—**In exercise of the powers conferred by clause (za) of sub-section (2) of Section 87, read with sub-section (3) of Section 69B 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 or 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 the Secretary to the Government of India in the Department of Information Technology under the Ministry of Communications and Information Technology;

(e) "computer resource" means computer resource 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 unauthorized access, denial of service/ disruption, unauthorised use of a computer resource 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 resource;

(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 variations and cognate expressions, includes to view or inspect or record or collect traffic data or information generated, transmitted, received or stored in a computer resource 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 419A of the Indian Telegraph Rules, 1951;

(o) "security policy" means documented business rules and processes for protecting information and the computer resource,

(p) "traffic data" means traffic data as defined in Explanation (ii) to Section 69B of the Act.

**3. Directions for monitoring.—**(1) No directions for monitoring and collection of traffic data or information under sub-section (3) of Section 69B of the Act shall be issued, except by an order made by the competent authority.

(2) The competent authority may issue directions for monitoring for any or all of the following purposes related to cyber security, namely:—

(a) forecasting of imminent cyber incidents;

(b) monitoring network application with traffic data or information on computer resource;

(c) identification and determination of viruses or computer contaminant;

(d) tracking cyber security breaches or cyber security incidents;

(e) tracking computer resource 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 resource as a part of investigation or internal audit of information security practices in the computer resource;

(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 collection 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 email 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 directions 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 resource 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 of 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 thereunder 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 findings whether the directions issued under sub-rule (2) of rule 3 are in accordance with the provisions of sub-section (3) of Section 69B 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 destroy 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 authorises 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 resource by the employee 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 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 internal audit; or

(vi) accessing or analysing 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 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 provisions 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 authorised 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.