Draft Rules under section 69 of the Information Technology (Amendment) Act, 2008

Ministry of Communications and Information Technology
(Department of Information Technology)
New Delhi , Dated ------

G.S.R ---- In exercise of the powers conferred by clause (y) of sub-section (2) of section 87, read with sub-section (2) of section 69 of the Information Technology Act, 2000, as amended by the Information Technology (Amendment) Act, 2008 (10 of 2009), the Central Government hereby makes the following rules, namely:

1. (1) These rules may be called the Information Technology (Directions for Interception, Monitoring and Decryption of 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, as amended by the Information Technology (Amendment) Act, 2008;

(b) "Computer resource" means computer resource as defined in section 2(1)(k) of the Information Technology Act, 2000;

(c) "Decryption" means the process of conversion of information in non-intelligible form to an intelligible information via a mathematical formula, code, password or algorithm;

(d) "Decryption assistance" means to –
  (i) allow access, to the extent possible, to encrypted information; or
  (ii) facilitate conversion of encrypted information into an intelligible form;

(e) "Decryption direction" means a direction issued under Rule (3) in terms of which a decryption key holder is directed to –
  (i) disclose a decryption key; or
  (ii) provide decryption assistance in respect of encrypted information

(f) "Decryption key" means any key, mathematical formula, code, password, algorithm or any other data which is used to -
  (i) allow access to encrypted information: or
  (ii) facilitate the conversion of encrypted information into an intelligible form;

(g) "Decryption key holder" means any person who is in possession of a decryption key for purposes of subsequent decryption of encrypted information relating to direct or indirect communications;

(h) "Information" means information as defined in section 2(1)(v) of the Information Technology Act, 2000;

(i) "Intercept" with its grammatical variations and cognate expressions, means the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the -

  (a) monitoring of any such communication by means of a monitoring device;

  (b) viewing, examination or inspection of the contents of any direct or indirect communication; and

  (c) diversion of any direct or indirect communication from its intended destination to any other destination;

(j) "Interception 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 or in combination with any other instrument, device, equipment or apparatus, to intercept any communication;

and a reference to an "interception device" includes, where applicable, a reference to a "monitoring device";

(k) "Intermediary" means an intermediary as defined in section 2(1) of the Information Technology (Amendment) Act, 2008;

(l) "Monitor" with its grammatical variations and cognate expressions, includes to view or to inspect or listen to or record information by means of a monitoring device;

(m) "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 to inspect or to listen to or record any information;

(n) "Review Committee" means a Review Committee as constituted in Rule 419A of Indian Telegraph (Amendment) Rules, 2007.

3. Directions for interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource under sub-section (2) of section 69 of the Information Technology (Amendment) Act, 2008 (hereinafter referred to as the said Act) shall not be issued except by an order made by the concerned competent authority who is Union Home Secretary in case of Government of India; the Secretary in-charge of Home Department in a State Government or Union Territory as the case may be. In unavoidable circumstances, such order may be made by an officer, not below the rank of a Joint Secretary to the

Government of India, who has been duly authorised by the Union Home Secretary or by an officer equivalent to rank of Joint Secretary to Government of India duly authorised by the Secretary in-charge of Home Department in the State Government or Union Territory, as the case may be:

Provided that in emergency cases –

(i)) in remote areas, where obtaining of prior directions for interception or monitoring or decryption of information is not feasible; or

(ii) for operational reasons, where obtaining of prior directions for interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource is not feasible;

the required interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource shall be carried out with the prior approval of the Head or the second senior most officer of the Security and Law Enforcement Agencies (hereinafter referred to as the said Security Agencies) at the Central Level and the officers authorised in this behalf, not below the rank of Inspector General of Police or an officer of equivalent rank, at the State and Union Territory level. The concerned competent authority, however, shall be informed of such interceptions or monitoring or decryption by the approving authority within three working days and that such interceptions or monitoring or decryption shall be got confirmed by the concerned competent authority within a period of seven working days. If the confirmation from the concerned competent authority is not received within the stipulated seven working days, such interception or monitoring or decryption shall cease and the same information shall not be intercepted or monitored or decrypted thereafter without the prior approval of the concerned competent authority, as the case may be.

4. The competent authority may authorize any agency of the Government to intercept, monitor or decrypt information generated, transmitted, received or stored in any computer resource for the purpose given in sub-section (1) of section 69 of the Act.

5. The competent authority under Rule (3) shall have the power to give decryption direction to the decryption key holder for decryption of any information involving a computer resource or part thereof.

6. Notwithstanding anything contained in Rule (3) for the purposes of any interception or monitoring or decryption of information, if such interception or monitoring or decryption of information involves interception or monitoring or decryption of information beyond State’s or Union Territory’s jurisdiction, the Secretary

in-charge of the Home Department in the State or Union Territory, as the case may be, shall make a request to the Union Home Secretary for issuing direction to the appropriate authority for any such interception or monitoring or decryption of information.

7. Any direction issued by the concerned competent authority under Rule (3) 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.

8. While issuing directions under Rule (3) the concerned competent authority shall consider possibility of acquiring the necessary information by other means and the directions under Rule (3) shall be issued only when it is not possible to acquire the information by any other reasonable means.

9. The interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource so directed shall be the interception or monitoring or decryption of any information as is sent to or from any person or class of persons or relating to any particular subject whether such information or class of information are received with one or more computer resources specified in the direction, being a computer resource likely to be used for the generation, transmission, receiving, storing of information from or to one particular person specified or described in the direction or one or many set of premises specified or described in the direction.

10. The directions under Rule (3) shall specify the name and designation of the officer or the agency to whom the intercepted or monitored or decrypted or stored information is to be disclosed and also specify that the use of intercepted or monitored or decrypted information shall be subject to the provisions of sub-section (2) of section 69 of the said Act.

11. The directions for interception or monitoring or decryption under Rule (3) shall remain in force, unless revoked earlier, for a period not exceeding sixty days from the date of issue and may be renewed but same shall not remain in force beyond a total period of one hundred and eighty days.

12. The agency authorised by the competent authority under Rule (3) shall designate one or more nodal officers not below the rank of Superintendent of Police or Additional Superintendent of Police or the officer of the equivalent rank to authenticate and send the requisitions conveying direction issued under Rule (3) for interception or monitoring or decryption to the designated officers of the concerned intermediaries or person in-charge of computer resource. Such requisition shall be delivered to the

designated officer of the concerned intermediary by an officer not below the rank of Inspector of Police or officer of equivalent rank.

13. The officer issuing the requisition conveying direction for interception or monitoring or decryption under Rule (3) shall also make a request in writing to the designated officers of intermediaries or person in-charge of computer resources, who shall extend all facilities, co-operation and assistance for interception or monitoring or decryption mentioned in the directions.

14. The intermediaries or person in-charge of computer resource shall designate separate officer to receive requisition and to handle such requisition from the nodal officer for interception or monitoring or decryption of information generated, transmitted, received or stored in any computer resource.

15. The designated officers of the intermediaries or person in-charge of computer resources shall acknowledge the instructions received by way of letters/fax/ electronically signed email to the nodal officer of the concerned agencies within two hours on receipt of intimation for interception or monitoring or decryption of information.

16. The designated officer of intermediary or person in-charge of computer resource authorised to intercept or monitor or decrypt any information shall maintain proper records mentioning therein, the intercepted or monitored or decrypted information, the particulars of persons, computer resource, email account(s), website address etc. whose information has been intercepted or monitored or decrypted, the name and other particulars of the officer or the authority to whom the intercepted or monitored or decrypted information has been disclosed, the number of copies, including corresponding electronic records of the intercepted or monitored or decrypted information made and the mode or the method by which such copies, including corresponding electronic record are made, the date of destruction of the copies, including corresponding electronic record and the duration within which the directions remain in force.

17. If a decryption direction or a copy thereof is handed to the decryption key holder to whom the decryption direction is addressed by the nodal officer as prescribed in Rule (12), the decryption key holder concerned must within the period stated in the decryption direction –

(a) disclose the decryption key; or

(b) provide the decryption assistance

specified in the decryption direction concerned to the authorised person concerned.

18. The designated officers of the intermediaries or person in-charge of computer resources shall forward every fifteen days a list of interception or monitoring or decryption authorizations received by them during the preceding fortnight to the nodal officers of the agencies authorised under Rule (3) for confirmation of the authenticity of such authorizations. The list should include details such as the reference and date of orders of the concerned competent authority such as Union Home Secretary or Secretary in-charge of the Home Department in the State Government or Union Territory including orders issued under emergency cases, date and time of receipt of such orders and the date and time of implementation of such orders.

19. The intermediary or the person in-charge of the computer resource so directed under Rule (3) shall provide technical assistance and the equipment wherever requested by the agency authorized under Rule (3) for performing an act of interception or monitoring or decryption including for the purposes of:-

(i) the installation of equipment of the agency authorised under Rule (3) for the purposes of interception or monitoring or decryption or accessing stored information in accordance with directions by the nodal officer under Rule (3); or

(ii) the maintenance, testing or use of such equipment; or

(iii) the removal of such equipment; or

(iv) the performance of any act required for accessing of stored information under the direction issued by the competent authority under Rule (3).

20. The intermediaries or person in-charge of computer resources shall put in place adequate and effective internal checks to ensure the unauthorised interception of messages does not take place and extreme secrecy is maintained and utmost care and precaution is taken in the matter of interception or monitoring or decryption of information as it affects privacy of citizens and also that this matter is handled only by the designated officers of the intermediary and no other person of the intermediary shall have access to such intercepted or monitored or decrypted information.

21. The intermediaries or person in-charge of computer resources are responsible for their respective actions of their employees also. In case of established violations pertaining to maintenance of secrecy and confidentiality of information and unauthorised interception or monitoring or decryption of information, action shall be taken against the intermediaries or person in-charge of computer resources under the relevant provisions of the laws of the country.

22. The Review Committee shall meet at least once in two months and record its findings whether the directions issued under Rule (3) are in accordance with the provisions of sub-section (2) of section 69 of the Act. When 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 order for destruction of the copies, including corresponding electronic record of the intercepted or monitored or decrypted information.

23. Records, including electronic records pertaining to such directions for interception or monitoring or decryption of information and of intercepted or monitored or decrypted information shall be destroyed by the relevant Security Agencies every six months unless these are, or likely to be, required for functional requirements.

24. The intermediaries or person in-charge of computer resources shall destroy records pertaining to directions for interception of information within two months of discontinuance of the interception or monitoring or decryption of such information and in doing so they shall maintain extreme secrecy.

25. Any person who intentionally, without authorisation under Rule (3) and Rule (4), intercepts or attempts to intercept, or authorises or assists any other person to intercept or attempts to intercept any information in the course of its occurrence or transmission at any place within India, shall be proceeded against under the relevant provisions of the Law.

26. Any interception, monitoring or decryption of 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, undertaken in course of his duty relating to the services provided by that intermediary, shall not be unlawful, if such activities are reasonably necessary for the discharge his duties as per the prevailing industry practices, in connection with :

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 code 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.

27. The contents of intercepted or monitored or stored or decrypted information shall not be used or disclosed by intermediary or any of its employees or person in-charge of computer resource to any person other than the intended recipient of the said information under Rule (10). Any intermediary or its employees or person in-charge of computer resource who contravenes these provisions shall be proceeded against under the relevant provisions of the Act.

28. The contents of intercepted or monitored or decrypted information shall not be used or disclosed by the agency authorised under Rule (3) for any other purpose, except for investigation or sharing with other Security Agencies for the purpose of investigation or in judicial proceedings before the competent court.

29. Save as otherwise provided in Rule (28), the contents of intercepted or monitored or decrypted information shall not be disclosed or reported in public by any means, without the order of the competent Indian court.

30. Save as otherwise provided in Rule (28), strict confidentiality shall be maintained in respect of direction for interception, monitoring or decryption issued by concerned competent authority and nodal officers under Rule (3).

31. Whenever asked for by the concerned Security agency at the Centre, security agencies at the State and the Union Territories level must promptly share any information which these agencies may have obtained following directions for interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource under Rule (3), with the Security agencies at the Centre.