रजिस्ट्री सं० डी० एल०-33004/99 REGD. NO. D. L.-33004/99

भारत का राजपत्र
The Gazette of India

असाधारण
EXTRAORDINARY
भाग II—खण्ड 3—उप-खण्ड (i)
PART II—Section 3—Sub-section (i)
प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 618] नई दिल्ली, मंगलवार, अक्तूबर 27, 2009/कार्तिक 5, 1931
No. 618] NEW DELHI, TUESDAY, OCTOBER 27, 2009/KARTIKA 5, 1931

संचार और सूचना प्रौद्योगिकी मंत्रालय

(सूचना प्रौद्योगिकी विभाग)

अधिसूचना

नई दिल्ली, 27 अक्तूबर, 2009

सा.का.नि. 778(अ).— केंद्रीय सरकार, केंद्रीय सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 52 के साथ पठित धारा 87 की उपधारा (2) के खंड (द) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए और साइबर विनियमन अपील अधिकरण (पीठासीन अधिकारी के वेतन, भत्ते और सेवा के अन्य निबंधन एवं शर्तें) नियम, 2003 को उन बातों के सिवाय अधिक्रांत करते हुए, जिन्हें ऐसे अधिक्रमण के पूर्व किया गया है या करने से लोप किया गया है, साइबर अपील अधिकरण के अध्यक्ष और सदस्यों की सेवा के निबंधनों और शर्तों को विनियमित करने के लिए निम्नलिखित नियम बनाती है, अर्थात् :—

1. **संक्षिप्त नाम और प्रारंभ**--(1) इन नियमों का संक्षिप्त नाम साइबर अपील अधिकरण (अध्यक्ष और सदस्यों के वेतन, भत्ते और सेवा के अन्य निबंधन तथा शर्तें) नियम, 2009 है ।

(2) ये राजपत्र में प्रकाशन की तारीख को प्रवृत्त होंगे ।

2. **परिभाषाएं**— (1) इन नियमों में, जब तक कि संदर्भ से अन्यथा अपेक्षित न हो,—

(क) ''अधिनियम'' से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है ;

(ख) ''साइबर अपील अधिकरण'' से अधिनियम की धारा 48 की उपधारा (1) के अधीन स्थापित साइबर अपील अधिकरण अभिप्रेत है ;

(ग) ''अध्यक्ष'' से अधिनियम की धारा 49 के अधीन नियुक्त साइबर अपील अधिकरण का अध्यक्ष अभिप्रेत है ;

(घ) ''सदस्य'' से अधिनियम की धारा 49 के अधीन नियुक्त साइबर अपील अधिकरण का सदस्य अभिप्रेत है ;

(2) उन सभी शब्दों और पदों के, जो इन नियमों में प्रयुक्त हैं और परिभाषित नहीं हैं किंतु अधिनियम में परिभाषित है, क्रमशः वही अर्थ होंगे, जो अधिनियम में उनके है ।

3. वेतन और भत्ते– (1) अध्यक्ष और सदस्य को ऐसा वेतन और भत्ते संदत्त किए जाएंगे, जो भारत सरकार के सचिव को अनुज्ञेय हैं, जिनके अंतर्गत वे सभी प्रसुविधाएं भी हैं, जिनका सचिव हकदार है :

परंतु, यथास्थिति, अध्यक्ष या सदस्य के रूप में किसी ऐसे व्यक्ति की नियुक्ति की दशा में, जो उच्चतम न्यायालय या किसी उच्च न्यायालय के न्यायाधीश के रूप में सेवानिवृत्त हुआ है या जो केंद्रीय सरकार या किसी राज्य सरकार के अधीन सेवा से निवृत्त हुआ है और जो पेंशन, उपदान, अंशदायी भविष्यनिधि में नियोजक के अंशदान के रूप में किन्हीं सेवानिवृत्ति फायदों या अन्य प्रकार के सेवानिवृत्ति फायदों को प्राप्त कर रहा है या प्राप्त कर चुका है या प्राप्त करने का हकदार हो गया है, यथास्थिति ऐसे अध्यक्ष या सदस्य के वेतन में से पेंशन अथवा अंशदायी भविष्यनिधि में नियोजक के अंशदान अथवा किसी अन्य प्रकार के सेवानिवृत्ति फायदों की, यदि कोई हों, जो उसके द्वारा लिए गए हैं या लिए जाने वाले हों, सकल राशि को कम कर दिया जाएगा :

परंतु यह और कि यदि किसी उच्चतम न्यायालय या किसी उच्च न्यायालय के सेवानिवृत्त न्यायाधीश को यथास्थिति अध्यक्ष या सदस्य के रूप में नियुक्त किया जाता है तो ऐसे अध्यक्ष या सदस्य की सेवा के निबंधन और शर्तें विभिन्न अधिकरणों में न्यायाधीशों की नियुक्ति के संबंध में वित्त मंत्रालय द्वारा जारी किए गए निर्देशों के अनुसार होंगी तथा उन्हें उस मंत्रालय के परामर्श से तय किया जाएगा ।

4. छुट्टी– अध्यक्ष और सदस्य ऐसी छुट्टी के लिए हकदार होंगे जो भारत सरकार के सचिव को अर्जित छुट्टी, अर्ध-वेतन छुट्टी, असाधारण छुट्टी, परिवर्तित छुट्टी और आकस्मिक छुट्टी के संबंध में लागू है ।

5. छुट्टी मंजूर करने वाला प्राधिकारी– सचिव, सूचना प्रौद्योगिकी विभाग, संचार और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार अध्यक्ष और सदस्य को छुट्टी मंजूर करने के लिए सक्षम प्राधिकारी होगा ।

6. पेंशन या भविष्यनिधि– (1) यदि उच्चतम न्यायालय या किसी उच्च न्यायालय का कोई सेवारत न्यायाधीश या भारतीय विधि सेवा का कोई सदस्य, अध्यक्ष या सदस्य के पद पर नियुक्त किया जाता है, तो अधिकरण में की गई सेवा उस सेवा के, जिससे वह संबंधित है, नियमों के अनुसार ली जाने वाली पेंशन के लिए गणना में ली जाएगी और वह साधारण भविष्यनिधि (केंद्रीय सेवाएं) नियम, 1960 के उपबंधों द्वारा भी शासित होगा ।

(2) सभी अन्य मामलों में, अध्यक्ष ओर सदस्य अंशदायी भविष्यनिधि (भारत) नियम, 1962 के उपबंध द्वारा शासित होंगे ।

7. यात्रा और दैनिक भत्ते– यथास्थिति, अध्यक्ष या सदस्य, जब दौरे पर हों (जिसके अंतर्गत अधिकरण में उसकी पदावधि की समाप्ति पर अपने गृह नगर जाने के लिए की गई यात्रा भी है) यात्रा भत्ते, दैनिक भत्ते, घरेलू वस्तुओं के परिवहन और इसी प्रकार के अन्य मामलों के लिए उन्हीं दरों पर हकदार होंगे जो भारत सरकार के सचिव को लागू हैं ।

8. छुट्टी यात्रा रियायत– अध्यक्ष और सदस्य छुट्टी यात्रा रियायत का उन्हीं दरों पर, उपभोग करने के लिए हकदार होंगे, जो भारत सरकार के सचिव को अनुज्ञेय हैं ।

9. वाहन की सुविधा–अध्यक्ष और सदस्य भारत सरकार के सचिव द्वारा टैक्सी किराये पर लेने के लिए तत्समय प्रवृत्त नियमों और आदेशों के अनुसार पूर्णकालिक आधार पर टैक्सी किराये पर लेने के लिए हकदार होंगे ।

10. मकान किराया भत्ता–अध्यक्ष और सदस्य उसी दर पर मकान किराया भत्ते के लिए हकदार होंगे जो तत्समय समतुल्य वेतन और श्रेणी वेतन प्राप्त करने वाले केंद्रीय सरकार के समूह 'क' अधिकारियों को अनुज्ञेय है ।

11. चिकित्सा उपचार के लिए सुविधाएं–अध्यक्ष और सदस्य ऐसे चिकित्सा उपचार और अस्पताल सुविधाओं के लिए हकदार होंगे जो केंद्रीय सरकार स्वास्थ्य स्कीम नियम, 1954 में उपबंधित है और उन स्थानों पर जहां केंद्रीय सरकार स्वास्थ्य स्कीम प्रवृत्त नहीं है, वहां उक्त अध्यक्ष और सदस्य उन सुविधाओं के हकदार होंगे जो केंद्रीय सेवा (चिकित्सीय परिचर्या) नियम, 1944 में उपबंधित हैं ।

12. पद और गोपनीयता की शपथ–यथास्थिति, अध्यक्ष या सदस्य के रूप में नियुक्त प्रत्येक व्यक्ति अपना पद ग्रहण करने के पूर्व, इन नियमों से उपाबद्ध क्रमशः प्ररूप 1 और प्ररूप 2 में अपने पद और गोपनीयता की शपथ लेगा और हस्ताक्षर करेगा ।

13. वित्तीय और अन्य हित की घोषणा-- प्रत्येक व्यक्ति, यथास्थिति, अध्यक्ष या सदस्य के रूप में अपनी नियुक्ति पर, इन नियमों से उपाबद्ध प्ररूप 3 में, केंद्रीय सरकार के समाधानप्रद रूप में, एक घोषणा देगा कि वह कोई ऐसा वित्तीय या अन्य हित नहीं रखता है, जिससे, यथास्थिति, अध्यक्ष या सदस्य के रूप में उसके कृत्यों पर प्रतिकूल प्रभाव पड़ने की संभावना है ।

14. अवशिष्ट उपबंध–अध्यक्ष और सदस्य की सेवा की शर्तों से संबंधित ऐसा कोई विषय, जिसके संबंध में इन नियमों में कोई स्पष्ट उपबंध नहीं किया गया है, उन नियमों के अनुसार होगा, जो समतुल्य वेतन और श्रेणी वेतन लेने वाले केंद्रीय सरकार के समूह 'क' अधिकारियों को लागू हैं ।

प्ररूप - 1

(नियम 12 देखिए)

साइबर अपील अधिकरण के अध्यक्ष/सदस्यों के लिए पद की शपथ का प्ररूप

मैं.. जो अध्यक्ष/सदस्य (उस भाग को काट दें, जो लागू नहीं है) नियुक्त हुआ हूं, सत्यनिष्ठा से प्रतिज्ञान करता हूं और ईश्वर की शपथ लेता हूं कि मैं साइबर अपील अधिकरण के अध्यक्ष/सदस्य (वह भाग काट दें जो लागू नहीं है) के रूप में अपने कर्तव्यों का अपनी पूरी योग्यता, ज्ञान और विवेक से, भय या पक्षपात, अनुराग या द्वेष के बिना, श्रद्धापूर्वक और शुद्ध अंतःकरण से निर्वहन करूंगा ।

(अध्यक्ष/सदस्य का नाम)

साइबर अपील अधिकरण

तारीख :

स्थान :

प्ररूप - 2

(नियम 12 देखिए)

साइबर अपील अधिकरण के अध्यक्ष/सदस्यों के लिए गोपनीयता की शपथ का प्ररूप

मैं.. जो अध्यक्ष/सदस्य (उस भाग को काट दें जो लागू नहीं है) के रूप में नियुक्त हुआ हूं, सत्यनिष्ठा से प्रतिज्ञान करता हूं और ईश्वर की शपथ लेता हूं कि मैं जो कोई विषय, अध्यक्ष/सदस्य (उस भाग को काट दें जो लागू नहीं है) मेरे विचार के लिए लाया जाएगा अथवा मुझे ज्ञात होगा, उसे किसी व्यक्ति या व्यक्तियों को, तब के सिवाए जबकि के रूप में अपने कर्तव्यों के सम्यक निवर्हन के लिए ऐसा करना अपेक्षित हो, मैं प्रत्यक्ष अथवा अप्रत्यक्ष रूप से संसूचित या प्रकट नहीं करूंगा ।

(अध्यक्ष/सदस्य का नाम)

साइबर अपील अधिकरण

तारीख :

स्थान :

प्ररूप - 3

(नियम 13 देखिए)

किसी प्रतिकूल वित्तीय या अन्य हित के अर्जन के विरुद्ध घोषणा

मैं.. जो साइबर अपील अधिकरण के अध्यक्ष/सदस्य (उस भाग को काट दें जो लागू नहीं है) के रूप में नियुक्त हुआ हूं, सत्यनिष्ठा से प्रतिज्ञान करता हूं और घोषणा करता हूं कि मैं ऐसा कोई वित्तीय या अन्य हित नहीं रखता हूं, न भविष्य में रखूंगा जिससे साइबर अपील अधिकरण के अध्यक्ष/सदस्य (उस भाग को काट दें जो लागू नहीं है) के रूप मेरे कृत्य करने पर प्रतिकूल प्रभाव पड़ने की संभावना हो ।

(अध्यक्ष/सदस्य का नाम)

साइबर अपील अधिकरण

तारीख :

स्थान :

[सं. 9(16)/2004-ई.सी.]

एन. रवि शंकर, संयुक्त सचिव

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(Department of Information Technology)

NOTIFICATION

New Delhi, the 27th October, 2009

G.S.R. 778(E)— In exercise of the powers conferred by clause (r) of sub-section (2) of Section 87, read with section 52 of the Information Technology Act 2000 (21 of 2000), and in supersession of the Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003, except as respects things done or omitted to be done before such supersession, the Central Government hereby makes the following rules regulating the terms and conditions of the service of the Chairperson and Members of the Cyber Appellate Tribunal, namely:--

1. Short title and commencement.—(1) These rules may be called the Cyber Appellate Tribunal (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Rules, 2009.

(2) They shall come into force on the date of their publications in the Official Gazette.

2. Definitions.— (1) In these rules, unless the context otherwise requires,—

(a) "Act" means Information Technology Act, 2000 (21 0f 2000);
(b) "Cyber Appellate Tribunal" means the Cyber Appellate Tribunal established under sub-section (1) of section 48 of the Act;
(c) "Chairperson" means the Chairperson of the Cyber Appellate Tribunal appointed under section 49 of the Act;
(d) "Member" means the Member of the Cyber Appellate Tribunal appointed under section 49 of the Act;

(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. Salary and allowances.— (1) The Chairperson and the Member shall be paid such salary and allowances, as are admissible to a Secretary to the Government of India, including all the benefits that a Secretary is entitled to:

Provided that in the case of appointment of a person as the Chairperson or the Member, as the case may be, who has retired as a Judge of the Supreme Court or a High Court or who has retired from service under the Central Government or a State Government and who is in receipt of, or has received, or has become entitled to receive any retirement benefits by way of pension, gratuity, employer's contribution to Contributory Provident Fund or other forms of retirement benefits, the pay of such Chairperson or the Member, as the case maybe, shall be reduced by the gross amount of pension or employer's contribution to the Contributory Provident Fund or any other form of retirement benefit, if any, drawn or to be drawn by him:

Provided further that in case a retired Judge of a Supreme Court or a High Court is appointed as the Chairperson or the Member, as the case maybe, the terms and conditions of service of such Chairperson or Member shall be in accordance with the instructions issued by the Ministry of Finance in respect of appointment of Judges to various Tribunals and in consultation with that Ministry.

4. Leave.— The Chairperson and the Member shall be entitled to leave as are applicable to the Secretary to the Government of India in respect of earned leave, half pay leave, extraordinary leave, commutation of leave and casual leave.

5. Leave sanctioning authority.— The Secretary, Department of Information Technology, Ministry of Communications and Information Technology, Government of India, shall be the authority competent to sanction leave to the Chairperson and the Member.

6. Pension or Provident Fund.— (1) In case a serving Judge of the Supreme Court or a High Court or a member of the Indian Legal Service is appointed to the post of the Chairperson or the Member, the service rendered in the Tribunal shall count for pension, to be drawn in accordance with the rules of the service to which he belongs, and he shall also be governed by the provisions of the General Provident Fund (Central Services) Rules, 1960.

(2) In all other cases, the Chairperson and the Member shall be governed by the provision of the Contributory Provident Fund (India) Rules, 1962.

7. Travelling and daily allowances.— The Chairperson or the Member, as the case may be, while on tour (including the journey undertaken on the expiry of his term in the Tribunal to proceed to his home town) shall be entitled to the travelling allowance, daily allowance, transportation of personal effects and other similar matters at the same rates as are applicable to the Secretary to the Government of India.

8. Leave travel concession.—The Chairperson and the Member shall be entitled to avail leave travel concession at the same rates as are admissible to the Secretary to the Government of India.

9. Facility of conveyance.— The Chairperson and the Member shall be entitled to hire a taxi on whole time basis in accordance with the rules or orders for the time being in force for hire of taxi by the Secretary to the Government of India.

10. House rent allowance.—The Chairperson and the Member shall be entitled to house rent allowance at the same rate as are, for the time being, admissible to Group 'A' officers of the Central Government drawing equivalent pay and grade pay.

11. Facilities for medical treatment.— The Chairperson and the Member shall be entitled to medical treatment and hospital facilities, as provided in the Central Government Health Scheme Rules, 1954 and in places where the Central Government Health Scheme is not in operation, the said Chairperson and the Member shall be entitled to the facilities as provided in the Central Services (Medical Attendance) Rules, 1944.

12. Oath of office and secrecy.— Every person appointed as the Chairperson or the Member, as the case may be, shall, before entering upon his office, make and subscribe an oath of office and secrecy, in Form I and Form II respectively annexed to these rules.

13. Declaration of financial or other interest.— Every person, on his appointment as the Chairperson or the Member, as the case may be, shall give a declaration in Form III annexed to these rules, to the satisfaction of the Central Government, that he does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or the Member, as the case may be.

14. Residuary provision.— Any matter relating to the conditions of service of the Chairperson and the Member with respect to which no express provision has been made in these rules shall be as per the rules applicable to the Group 'A' officers of the Central Government drawing equivalent pay and grade pay.

FORM – I
(See rule 12)

Form of Oath of Office for the Chairperson/Members of the Cyber Appellate Tribunal

I, ___________________, having been appointed as the Chairperson/Member (*cross out portion not applicable*) do solemnly affirm and do swear in the name of God that I will faithfully and conscientiously discharge my duties as the Chairperson/Member (*cross out portion not applicable*), of the Cyber Appellate Tribunal, to the best of my ability, knowledge and judgement, without fear of favour, affection or ill-will.

Dated:

Place: (Name of the Chairperson/Member)
CYBER APPELLATE TRIBUNAL

FORM – II
(See rule 12)

Form of Oath of Secrecy for the Chairperson/Members of the Cyber Appellate Tribunal

I, ___________________, having been appointed as the Chairperson/Member (*cross out portion not applicable*) do solemnly affirm and swear in the name of God that I will not directly or indirectly communicate or reveal to any person or persons any matter which shall be brought under my consideration or shall become known to me as the Chairperson/ a Member (*cross out portion not applicable*), of the Cyber Appellate Tribunal except as may be required for the due discharge of my duties as the Chairperson/ a Member ((*cross out portion not applicable*).

Dated:
Place: (Name of the Chairperson/Member)
CYBER APPELLATE TRIBUNAL

FORM – III
(See rule 13)

Declaration against acquisition of any adverse financial or other interest

I, _______________, having been appointed as the Chairperson/Member (*cross out portion not applicable*) of Cyber Appellate Tribunal, do solemnly affirm and declare that I do not have, nor shall have in future any financial or other interest which is likely to affect prejudicially my functioning as the Chairperson /Member (*cross out portion not applicable*), of the Cyber Appellate Tribunal.

Dated: (Name of the Chairperson/Member)
CYBER APPELLATE TRIBUNAL

[No. 9(16)/2004-EC]
N. RAVI SHANKER, Jt. Secy.

अधिसूचना

नई दिल्ली, 27 अक्तूबर, 2009

सा.का.नि. 779(अ).— केंद्रीय सरकार, केंद्रीय सूचना प्रौद्योगिकी अधिनियम, 2000, (2000 का 21) की धारा 54 की उपधारा (3) के साथ पठित धारा 87 की उपधारा (2) के खंड (घ) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए और साइबर विनियमन अपील अधिकरण (पीठासीन अधिकारी के कदाचार या असमर्थता के अन्वेषण की प्रक्रिया) नियम, 2003 को उन बातों के सिवाय अधिक्रांत करते हुए, जिन्हें ऐसे अधिक्रमण के पूर्व किया गया है या करने से लोप किया गया है, निम्नलिखित नियम बनाती है, अर्थात् :

1. **संक्षिप्त नाम और प्रारंभ** – (1) इन नियमों का संक्षिप्त नाम साइबर अपील अधिकरण (अध्यक्ष और सदस्यों के कदाचार या असमर्थतता के अन्वेषण की प्रक्रिया) नियम, 2009 है ।

(2) ये राजपत्र में प्रकाशन की तारीख को प्रवृत्त होंगे ।

2. **परिभाषाएं**– (1) इन नियमों में, जब तक कि संदर्भ से अन्यथा अपेक्षित न हो,–

(क) ''अधिनियम'' से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है ;

(ख) ''अध्यक्ष'' से अधिनियम की धारा 49 के अधीन नियुक्त साइबर अपील अधिकरण का अध्यक्ष अभिप्रेत है ;

(ग) ''समिति'' से नियम 3 के उपनियम (2) के अधीन गठित कोई समिति अभिप्रेत है ;

(घ) ''सदस्य'' से अधिनियम की धारा 49 के अधीन नियुक्त साइबर अपील अधिकरण का सदस्य अभिप्रेत है ;

(ङ) ''अधिकरण'' से अधिनियम की धारा 48 की उपधारा (1) के अधीन स्थापित साइबर अपील अधिकरण अभिप्रेत है ।

(2) उन सभी अन्य शब्दों और पदों के, जो इन नियमों में प्रयुक्त है किंतु परिभाषित नहीं हैं, क्रमशः वही अर्थ होंगे जो अधिनियम में उनके है ।

3. **शिकायतों के अन्वेषण के लिए समिति.**– (1) यदि केंद्रीय सरकार द्वारा, यथास्थिति, अध्यक्ष या सदस्य के संबंध में उनके पद के कृत्यों के पालन में कदाचार या असमर्थतता का कोई निश्चित आरोप अभिकथित करने वाली कोई लिखित शिकायत प्राप्त की जाती है तो वह उस शिकायत की प्रारंभिक संवीक्षा करेगी ।

(2) यदि प्रारंभिक संवीक्षा पर, केंद्रीय सरकार अभिकथन के बारे में अन्वेषण करना आवश्यक समझती है तो वह उक्त शिकायत को ऐसी अन्य सामग्री सहित, जो उपलब्ध हो, उस समिति के समक्ष, शिकायत में किए गए अभिकथनों के आरोपों का अन्वेषण करने के लिए रखेगी, जो निम्नलिखित से मिलकर बनेगी, अर्थात् :

(i) सचिव (समन्वय और लोक शिकायत) मंत्रिमंडल सचिवालय, - अध्यक्ष ;

(ii) सचिव, सूचना प्रौद्योगिकी विभाग, भारत सरकार - सदस्य ;

(iii) सचिव, विधि कार्य विभाग, विधि और न्याय मंत्रालय, भारत सरकार - सदस्य

(3) समिति अन्वेषण की अपनी प्रक्रिया और पद्धति स्वयं बनाएगी, जिसमें नियम 4 के अधीन शिकायतकर्ता का साक्ष्य अभिलिखित करना और ऐसी सामग्री संग्रह करना, जो जांच के संचालन से सुसंगत हो, सम्मिलित हो सकेगा ।

(4) समिति ऐसी अवधि के भीतर, जो राष्ट्रपति द्वारा इस निमित विनिर्दिष्ट की जाएं, अपने निष्कर्ष, यथासंभवशीघ्र राष्ट्रपति को प्रस्तुत करेगी ।

4. **न्यायाधीश द्वारा जांच किया जाना.**– (1) यदि राष्ट्रपति की, नियम 3 के उपनियम (4) के अधीन समिति की रिपोर्ट की प्राप्ति पर, यह राय है कि, यथास्थिति, अध्यक्ष या सदस्य के कदाचार या असमर्थतता के किसी अभ्यारोपण की सत्यता के बारे में जांच करने के लिए युक्तियुक्त आधार हैं तो वह भारत के मुख्य न्यायमूर्ति को, जांच करने के लिए उच्चतम न्यायालय के किसी न्यायाधीश को नामनिर्दिष्ट करने का अनुरोध करते हुए एक निर्देश भेजेगी ।

(2) राष्ट्रपति, आदेश द्वारा, भारत के मुख्य न्यायमूर्ति द्वारा नामनिर्दिष्ट उच्चतम न्यायालय के न्यायाधीश को (जिसे इसमें इसके पश्चात् न्यायाधीश कहा गया है) जांच करने के प्रयोजन के लिए नियुक्त करेगी ।

(3) उपनियम (2) के अधीन न्यायाधीश की नियुक्ति की सूचना, यथास्थिति, अध्यक्ष या सदस्य को दी जाएगी ।

(4) राष्ट्रपति निम्नलिखित की एक प्रति न्यायाधीश को अग्रेषित करेगी–

(क) यथास्थिति, अध्यक्ष या सदस्य के विरुद्ध आरोपों की मदें और अभ्यारोपणों का कथन ;

(ख) साक्षियों का कथन, यदि कोई हो ; और

(ग) जांच से सुसंगत तात्विक दस्तावेज ।

(5) उपनियम (2) के अधीन नियुक्त न्यायाधीश ऐसे समय या अतिरिक्त समय के भीतर, जो राष्ट्रपति द्वारा विनिर्दिष्ट किया जाए, जांच पूरी करेगा ।

(6) यथास्थिति, अध्यक्ष या सदस्य को ऐसे समय के भीतर जो इस निमित न्यायाधीश द्वारा विनिर्दिष्ट किया जाए, प्रतिरक्षा का लिखित कथन प्रस्तुत करने का युक्तियुक्त अवसर दिया जाएगा ।

(7) जहां यह अभिकथित किया गया है कि, यथास्थिति, अध्यक्ष या सदस्य किसी शारीरिक या मानसिक असमर्थतता के कारण दक्षतापूर्वक अपने पद के कर्तव्यों का निर्वहन करने में असमर्थ है और अभिकथन से इन्कार किया जाता है, वहां न्यायाधीश, ऐसे चिकित्सा बोर्ड द्वारा, जो इस प्रयोजन के लिए राष्ट्रपति द्वारा नियुक्त किया जाए, यथास्थिति, अध्यक्ष या सदस्य की चिकित्सीय परीक्षा के लिए व्यवस्था कर सकेगा और, यथास्थिति, अध्यक्ष या सदस्य ऐसे समय के भीतर, जो इस निमित न्यायाधीश द्वारा विनिर्दिष्ट किया जाए, स्वयं को ऐसी चिकित्सीय परीक्षा के लिए प्रस्तुत करेगा ।

(8) चिकित्सा बोर्ड, यथास्थिति, अध्यक्ष या सदस्य की ऐसी चिकित्सीय परीक्षा करेगा, जो आवश्यक समझी जाए और न्यायाधीश को एक रिपोर्ट उसमें यह कथित करते हुए कि क्या असमर्थतता ऐसी है जो, यथास्थिति, अध्यक्ष या सदस्य को पद पर बने रहने में अयोग्य बनाती है, देगा ।

(9) यदि, यथास्थिति, अध्यक्ष या सदस्य ऐसी चिकित्सीय परीक्षा कराने से इन्कार करता है, जो चिकित्सा बोर्ड द्वारा आवश्यक समझी जाए, तो बोर्ड न्यायाधीश को एक रिपोर्ट, उसमें उस परीक्षा को कथित करते हुए, जिसे कराने से, यथास्थिति, अध्यक्ष या सदस्य ने इन्कार किया हो, देगा और न्यायाधीश, ऐसी रिपोर्ट की प्राप्ति पर, यह उपधारणा कर सकेगा कि, यथास्थिति, अध्यक्ष या सदस्य ऐसी शारीरिक या मानसिक असमर्थता से ग्रस्त है, जो उपनियम (4) के खंड (क) में निर्दिष्ट आरोपों की मद में अभिकथित की गई है ।

(10) न्यायाधीश, यथास्थिति अध्यक्ष या सदस्य के लिखित कथन और चिकित्सा बोर्ड की रिपोर्ट पर, यदि कोई हो, विचार करने के पश्चात् उपनियम (4) के खंड (क) में निर्दिष्ट आरोपों की मद का संशोधन कर सकेगा और ऐसे मामले में, यथास्थिति, अध्यक्ष या सदस्य को प्रतिरक्षा का नया लिखित कथन प्रस्तुत करने का युक्तियुक्त अवसर दिया जाएगा ।

(11) केंद्रीय सरकार उस सरकार के किसी अधिकारी या किसी अधिवक्ता को न्यायाधीश के समक्ष, यथास्थिति, अध्यक्ष या सदस्य के विरुद्ध मामला प्रस्तुत करने के लिए नियुक्त करेगी ।

(12) जहां केंद्रीय सरकार ने किसी अधिवक्ता को न्यायाधीश के समक्ष अपना मामला प्रस्तुत करने के लिए नियुक्त किया है, वहां, यथास्थिति, अध्यक्ष या सदस्य को भी उसके द्वारा चयन किए गए किसी अधिवक्ता द्वारा अपना मामला प्रस्तुत करने की अनुज्ञा दी जाएगी ।

5. इन नियमों के अधीन जांच करने के लिए विभागीय जांच (साक्षियों को हाजिर कराना तथा दस्तावेज पेश करना) अधिनियम, 1972 का लागू होना– विभागीय जांच (साक्षियों को हाजिर कराना तथा दस्तावेज पेश करना) अधिनियम, 1972 (1972 का 18) के उपबंध इन नियमों के अधीन की गई जांच को उसी प्रकार लागू होंगे, जैसे वे विभागीय जांचों को लागू होता है ।

6. न्यायाधीश की शक्तियां– न्यायाधीश, सिविल प्रक्रिया संहिता, 1908 (1908 का 5) में अधिकथित प्रक्रिया से आबद्ध नहीं होगा, किंतु नैसर्गिक न्याय के सिद्धांतों से मार्गदर्शित होगा और उसे अपनी प्रक्रिया को, जिसके अंतर्गत जांच के स्थान और समय नियत करना भी है, विनियमित करने की शक्ति होगी ।

7. अध्यक्ष या सदस्य का निलंबन.— राष्ट्रपति, नियम 4 में किसी बात के होते हुए भी और उक्त नियम के अनुसार की जा रही किसी कार्रवाई पर प्रतिकूल प्रभाव डाले बिना, आरोपों की गंभीरता को ध्यान में रखते हुए अधिकरण के, यथास्थिति उस अध्यक्ष या सदस्य को, जिसके विरुद्ध शिकायत अन्वेषण या जांच के अधीन है, निलंबित कर सकेगी ।

8. निर्वाह भत्ता.— निलंबनाधीन, यथास्थिति, अध्यक्ष या सदस्य को निर्वाह भत्ते का संदाय भारतीय प्रशासनिक सेवा के भारत सरकार के सचिव को तत्समय लागू नियमों और आदेशों के अनुसार विनियमित किया जाएगा ।

9. जांच रिपोर्ट.— अन्वेषण की समाप्ति के पश्चात्, न्यायाधीश राष्ट्रपति को अपनी रिपोर्ट प्रस्तुत करेगा, जिसमें आरोपों की प्रत्येक मद के संबंध में उसके निष्कर्षों और उनके लिए कारणों का, संपूर्ण मामले पर ऐसे संप्रेक्षणों सहित, जो वह ठीक समझे, कथन होगा ।

[सं. 9(16)/2004-ई.सी.]

एन. रवि शंकर, संयुक्त सचिव

NOTIFICATION

New Delhi, the 27th October, 2009

G.S.R. 779(E).— In exercise of the powers conferred by clause (s) of sub section (2) of section 87, read with subsection (3) of section 54 of the Information Technology Act 2000 (21 of 2000), and in supersession of the Cyber Regulations Appellate Tribunal (Procedure for Investigation of misbehaviour or Incapacity of Presiding Officer) Rules, 2003, except as respects things done or omitted to be done before such supersession, Central Government hereby makes the following rules, namely:—

1. Short title and commencement.— (1) These rules may be called the Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour or Incapacity of Chairperson and Members) Rules, 2009.

(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) "Chairperson" means the Chairperson of the Cyber Appellate Tribunal appointed under section 49 of the Act;

(b) "Committee" means a Committee constituted under sub–rule (2) of rule 3;

(c) "Member" means the Member of the Cyber Appellate Tribunal appointed under section 49 of the Act;

(d) "Tribunal" means the Cyber Appellate Tribunal established under sub-section (1) of section 48 of the Act.

(2) All other words and expressions used but not defined in these rules shall have the meaning respectively assigned to them in the Act.

3. Committee for investigation of complaints.— (1) If a written complaint, alleging any definite charges of misbehaviour or incapacity to perform the functions of the offices in respect of the Chairperson or the Member, as the case maybe, is received by the Central Government, it shall make a preliminary scrutiny of such complaint.

(2) If, on preliminary scrutiny, the Central Government considers it necessary to investigate into the allegation, it shall place the complaint together with other material as may be available, before a Committee consisting of the following officers to investigate the charges of allegations made in the complaint, namely :-

3855GI/09-2

(i) the Secretary (Co-ordination and Public Grievances) in the Cabinet Secretariat, Government of India - Chairman;

(ii) the Secretary, Department of Information Technology, Government of India – Member;

(iii) the Secretary, Department of Legal Affairs, Ministry of Law and Justice, Government of India -- Member.

(3) The Committee shall devise its own procedure and method of investigation, which may include recording of evidence of the complainant and collection of material under rule 4, which may be relevant to the conduct of inquiry.

(4) The Committee shall submit its findings to the President as early as possible within a period that may be specified by the President in this behalf.

4. Judge to conduct inquiry.— (1) If, the President, on receipt of the report of the Committee under sub-rule (4) of rule 3, is of the opinion that there are reasonable grounds for making an inquiry into the truth of any imputation of misbehaviour or incapacity of the Chairperson or the Member, as the case maybe, then, he shall make a reference to the Chief Justice of India requesting him to nominate a Judge of the Supreme Court to conduct the inquiry.

(2) The President shall, by order, appoint the Judge of the Supreme Court nominated by the Chief Justice of India (hereinafter referred to as the Judge) for the purpose of conducting the inquiry.

(3) Notice of appointment of the Judge under sub-rule (2) shall be given to the Chairperson or the Member, as the case may be.

(4) The President shall forward to the Judge a copy of—

(a) the articles of charges against the Chairperson or the Member, as the case maybe, and the statement of imputations;

(b) the statement of witnesses, if any; and

(c) material documents relevant to the inquiry.

(5) The Judge appointed under sub-rule (2) shall complete the inquiry within such time or further time as may be specified by the President.

(6) The Chairperson or the Member, as the case maybe, shall be given a reasonable opportunity of presenting a written statement of defence within such time as may be specified in this behalf by the Judge.

(7) Where it is alleged that the Chairperson or the Member, as the case maybe, is unable to discharge the duties of his office efficiently due to any physical or mental incapacity and the allegation is denied, the Judge may arrange for the medical examination of the Chairperson or the Member, as the case may be, by such Medical Board as may be appointed for the purpose by the President and the Chairperson or the Member, as the case may be, shall submit himself to such medical examination within the time specified in this behalf by the Judge.

(8) The Medical Board shall undertake such medical examination of the Chairperson or the Member, as the case may be, as may be considered necessary to and submit a report to the Judge stating therein whether the incapacity is such as to render the Chairperson or the Member, as the case maybe, unfit to continue in office.

(9) If the Chairperson or the Member, as the case maybe, refuses to undergo such medical examination as considered necessary by the Medical Board, the Board shall submit a report to the Judge stating therein the examination which the Chairperson or the Member, as the case maybe, has refused to undergo, and the Judge may, on receipt of such report, presume that the Chairperson or the Member, as the case may be, suffers from such physical or mental incapacity as is alleged in the article of charges referred to clause (a) of sub-rule (4).

(10) The Judge may, after considering the written statement of the Chairperson or the Member, as the case maybe, and report of the Medical Board, if any, amend the article of charges referred to in clause (a) of sub-rule (4) and in such case, the Chairperson or the Member, as the case maybe, shall be given a reasonable opportunity of presenting a fresh written statement of defence.

(11) The Central Government shall appoint an officer of that Government or an advocate to present the case against the Chairperson or the Member, as the case may be, before the Judge.

(12) Where the Central Government has appointed an advocate to present its case before the Judge, the Chairperson or the Member, as the case maybe, shall also be allowed to present his case by an advocate chosen by him.

5. Application of the Departmental Inquiries (Enforcement of Witness and Production of Documents) Act, 1972 to inquiries under these rules.— The provisions of the Departmental Inquiries (Enforcement of Witness and Rroduction of Documents) Act, 1972 (18 of 1972), shall apply to the inquiries made under these rules as they apply to departmental inquiries.

6. Powers of Judge.— The Judge shall not be bound by the procedure laid down in the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and shall have power to regulate his own procedure including the fixing of places and times of his inquiry.

7. Suspension of Chairperson or Member.-- Notwithstanding anything contained in rule 4, and without any prejudice to any action being taken in accordance with the said rule, the President, keeping in view the gravity of charges may suspend the Chairperson or the Member, as the case may be, of the Tribunal against whom a complaint is under investigation or inquiry.

8. Subsistence allowance.— The payment of subsistence allowance to a Chairperson or the Member, as the case may be, under suspension shall be regulated in accordance with the rules and orders for the time being applicable to a Secretary to the Government of India belonging to the Indian Administrative Service.

9. Inquiry Report.— After the conclusion of the investigation, the Judge shall submit his report to the President stating therein his findings and the reasons therefor on each of the articles of charges separately with such observations on the whole case as he thinks fit.

[No. 9(16)/2004-EC]
N. RAVI SHANKER, Jt. Secy.

अधिसूचना

नई दिल्ली, 27 अक्तूबर, 2009

सा.का.नि. 780(अ).— केंद्रीय सरकार, केंद्रीय सूचना प्रौद्योगिकी अधिनियम, 2000, (2000 का 21) की धारा 69 की उपधारा (2) के साथ पठित धारा 87 की उपधारा (2) के खंड (म) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए निम्नलिखित नियम बनाती है, अर्थात, :--

1. **संक्षिप्त नाम और प्रारंभ** – (1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (सूचना का अंतरोधन, मानीटर और विगूढ़न करने के लिए प्रक्रिया और रक्षोपाय) नियम, 2009 है ।

(2) ये राजपत्र में प्रकाशन की तारीख को प्रवृत्त होंगे ।

2. **परिभाषाएं**– इन नियम में, जब तक कि संदर्भ से अन्यथा अपेक्षित न हो,–

(क) ''अधिनियम'' से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है ;

(ख) ''संचार'' से सूचना या संकेत का किसी रीति से प्रसारण, पारेषण, वहन अभिप्रेत है और इसके अंतर्गत प्रत्यक्ष संचार और अप्रत्यक्ष संचार दोनों भी हैं ;

(ग) ''संचार लिंक'' से कंप्यूटर साधन का अंतः संयोजन करने के लिए सेटेलाइट, माइक्रोवेव, रेडियो, टेरेस्ट्रियल लाइन, तार, बेतार या किसी अन्य सूचना माध्यम का उपयोग अभिप्रेत है ;

(घ) ''सक्षम प्राधिकारी'' से निम्नलिखित अभिप्रेत है ;

(i) केंद्रीय सरकार की दशा में, गृहमंत्रालय का सचिव ; या

(ii) यथास्थिति, किसी राज्य सरकार या संघ राज्य क्षेत्र की दशा में गृह विभाग का भारसाधक सचिव

(ङ) ''कंप्यूटर साधन'' से अधिनियम की धारा 2 की उपधारा (1) के खंड (ट) में यथा परिभाषित कंप्यूटर साधन अभिप्रेत है ;

(च) ''विगूढ़न'' से अबोधगम्य रूप में सूचना के किसी बोधगम्य रूप में गणितीय सूत्र, कोड, संकेत शब्द या एलगोरिथ्म द्वारा या उनके किसी संयोजन द्वारा संपरिवर्तन की प्रक्रिया अभिप्रेत है ;

(छ) ''विगूढ़न सहायता'' से निम्नलिखित के लिए कोई सहायता अभिप्रेत है :-

(i) गूढ़ सूचना के लिए, संभव सीमा तक पहुंच अनुज्ञात करना ; या

(ii) गूढ़ सूचना का किसी बोधगम्य रूप में संपरिवर्तन सुकर बनाना ।

(ज) ''विगूढ़न निदेश'' से नियम 3 के अधीन जारी किया गया कोई ऐसा निदेश अभिप्रेत है, जिसमें विगूढ़न कुंजीधारक को -

(i) कोई विगूढ़न कुंजी प्रकट करने ; या

(ii) गूढ़ सूचना के संबंध में विगूढ़न सहायता प्रदान करने के लिए निदेशित किया जाता है ;

(झ) ''विगूढ़न कुंजी'' से कोई कुंजी, गणितीय सूत्र, कोड, संकेत शब्द, एलगोरिथ्म या ऐसा कोई अन्य डाटा अभिप्रेत है, जिसका,—

(i) गूढ़ सूचना के लिए पहुंच अनुज्ञात करने; या

(ii) गूढ़ सूचना का किसी बोध्यगम्य रूप में संपरिवर्तन सुकर बनाने ;

के लिए प्रयोग किया जाता है :-

(ञ) ''विगूढ़न कुंजीधारक'' से कोई ऐसा व्यक्ति अभिप्रेत है, जो विगूढ़न संबंधी यांत्रिकी का प्रभावी ढंग से उपयोग करता है और जिसके कब्जे में प्रत्यक्ष या अप्रत्यक्ष संचारों से संबंधित गूढ़ सूचना का पश्चात्‌वर्ती विगूढ़न करने के प्रयोजनों के लिए विगूढ़न कुंजी है ;

(ट) ''सूचना'' से अधिनियम की धारा 2 की उपधारा (1) के खंड (v) में यथा परिभाषित सूचना अभिप्रेत है ;

(ठ) ''अंतर्रुद्ध करना'' से, उसके व्याकरणिक रूपभेदों और सजातीय पदों सहित, किसी सूचना की अंर्तवस्तुओं का किसी साधन के उपयोग द्वारा, जिसके अंतर्गत कोई अंतर्रोधन युक्ति भी है, सुनना या अन्य अर्जन अभिप्रेत है, जिससे कि उस सूचना के भेजने वाले या उसे प्राप्त करने वाले या आशयित प्राप्त करने वाले से भिन्न किसी व्यक्ति को उस सूचना की कुछ या सभी अंतर्वस्तुओं को उपलब्ध कराया जा सके, और इसके अंतर्गत निम्नलिखित भी है -

(क) किसी ऐसी सूचना को मानीटर करने वाली युक्ति द्वारा मानीटर करना ;

(ख) किसी प्रत्यक्ष या अप्रत्यक्ष सूचना की अंर्तवस्तुओं को देखना, उनकी परीक्षा करना या निरीक्षण करना ; और

(ग) किसी प्रत्यक्ष या अप्रत्यक्ष सूचना का उसके आशयित गंतव्य स्थान से किसी दूसरे गंतव्य स्थान को परिवर्तन करना ;

(ड) ''अंतर्रोधन युक्ति'' से कोई इलेक्ट्रोनिक, यांत्रिक, इलेक्ट्रो-यांत्रिक, इलेक्ट्रो चुम्बकीय, प्रकाशकीय या अन्य उपकरण, युक्ति, उपस्कर या साधित्र, जिसका या तो स्वयं या किसी अन्य उपकरण, युक्ति, उपस्कर या साधित्र के संयोजन में किसी सूचना को अंतर्रुद्ध करने के लिए उपयोग किया जाता है या किया जा सकता है, अभिप्रेत है और किसी ''अंतर्रोधन युक्ति'' के प्रति किसी निर्देश में, जहां लागू हो, किसी ''मानीटरिंग युक्ति'' के प्रति निर्देश भी सम्मिलित है ;

(ढ) "मध्यवर्ती" से अधिनियम की धारा 2 की उपधारा (1) के खंड (ब) में यथा परिभाषित कोई मध्यवर्ती अभिप्रेत है ;

(ण) "मानीटर" के अंतर्गत, उसके व्याकरणिक रूपभेदों और सजातीय पदों सहित, मानीटर करने वाली युक्ति के द्वारा किसी सूचना को देखना या उसका निरीक्षण करना या उसे सुनना या अभिलिखित करना है ;

(त) "मानीटर करने वाली युक्ति" से अभिप्रेत है कोई इलेक्ट्रोनिक, यांत्रिक, इलेक्ट्रो-यांत्रिक, इलेक्ट्रो चुम्बकीय, प्रकाशकीय या अन्य उपकरण, युक्ति, उपस्कर या साधित्र, जिसका या तो स्वयं या किसी अन्य उपकरण, युक्ति, उपस्कर या साधित्र के संयोजन से किसी सूचना को देखने या उसका निरीक्षण करने या उसको सुनने या अभिलिखित करने के लिए उपयोग किया जाता है या उपयोग किया जा सकता है ;

(थ) "पुनर्विलोकन समिति" से भारतीय तार नियम, 1951 के नियम 419क के अधीन गठित पुनर्विलोकन समिति अभिप्रेत है ।

3. किसी सूचना को अंतर्रुद्ध या मानीटर या विगूढ़ित करने के लिए निदेश--कोई व्यक्ति, सक्षम प्राधिकारी द्वारा जारी किए गए किसी आदेश के सिवाय अधिनियम की धारा 69 की उपधारा (2) के अधीन किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त की गई या भंडारित किसी सूचना को अंतर्रुद्ध या मानीटर नहीं करेगा या उसका विगूढ़न नहीं करेगा :

परंतु किन्हीं अपरिहार्य परिस्थितियों में ऐसा आदेश किसी ऐसे अधिकारी द्वारा, जो भारत सरकार के संयुक्त सचिव की पंक्ति से नीचे की पंक्ति का न हो, जिसे सक्षम प्राधिकारी द्वारा सम्यक रूप से प्राधिकृत किया गया हो, जारी किया जा सकेगा :

परंतु यह और कि किसी आपात की दशा में--

(i) दूरस्थ क्षेत्रों में, जहां सूचना का अंतरोधन या मानीटर करने या विगूढ़न करने के लिए पूर्व निदेशों को प्राप्त करना साध्य नहीं है ; या

(ii) कार्यचालन संबंधी कारणों से, जहां किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त या भंडारित किसी सूचना को अंतर्रुद्ध या मानीटर करने या उसका विगूढ़न करने के लिए पूर्व निदेश प्राप्त करना साध्य नहीं है,

किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त या भंडारित किसी सूचना को केंद्रीय स्तर पर सुरक्षा और विधि प्रवर्तन अभिकरण (जिसे इसमें इसके पश्चात् उक्त सुरक्षा अभिकरण कहा गया है) के प्रमुख या ज्येष्ठतम अधिकारी के और राज्य या संघ राज्यक्षेत्र के स्तर पर इस निमित्त प्राधिकृत ऐसे अधिकारी के, जो पुलिस महानिरीक्षक की पंक्ति से नीचे की पंक्ति का न हो या समतुल्य पंक्ति का अधिकारी हो, पूर्व अनुमोदन से अंतर्रुद्ध, मानीटर या विगूढ़ित किया जा सकेगा :

परंतु यह भी कि वह अधिकारी, जिसने आपात की दशा में सूचना का अंतरोधन या मानीटर या विगूढ़न करने के लिए अनुमोदन दिया है, आपात के बारे में और ऐसा अंतरोधन या मानीटर या विगूढ़न करने के बारे में तीन कार्य दिवसों के भीतर सक्षम प्राधिकारी को लिखित रूप में सूचित करेगा और उस पर सात कार्य दिवसों की अवधि के भीतर सक्षम प्राधिकारी का अनुमोदन प्राप्त करेगा और यदि सक्षम प्राधिकारी का अनुमोदन सात कार्य दिवसों की उक्त अवधि के भीतर प्राप्त नहीं किया जाता है तो ऐसा अंतरोधन या मानीटर या विगूढ़न करना समाप्त हो जाएगा और सूचना को उसके पश्चात् सक्षम प्राधिकारी के पूर्व अनुमोदन के बिना अंतरोधित या मानीटर या विगूढ़ित नहीं किया जाएगा ।

(4) सरकार के अभिकरण को प्राधिकृत किय जाना--सक्षम प्राधिकारी सरकार के किसी अभिकरण को अधिनियम की धारा 69 की उपधारा (1) में विनिर्दिष्ट प्रयोजन के लिए किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त या भंडारित सूचना को अंतर्रुद्ध, मानीटर करने या उसका विगूढ़न करने के लिए प्राधिकृत कर सकेगा।

5. सक्षम प्राधिकारी द्वारा विगूढ़न निदेश का जारी किया जाना.-- सक्षम प्राधिकारी, नियम 3 के अधीन कंप्यूटर साधन या उसके भाग को अंतर्वलित करने वाली किसी सूचना के विगूढ़न के लिए विगूढ़न कुंजीधारक को कोई विगूढ़न निदेश दे सकेगा ।

6. किसी राज्य द्वारा अपनी अधिकारिता से परे सूचना का अंतरोधन या मानीटर या विगूढ़न किया जाना.— नियम 3 में अंतर्विलित किसी बात के होते हुए भी,यदि कोई राज्य सरकार या संघ राज्य क्षेत्र प्रशासन अपनी राज्य क्षेत्रीय अधिकारिता से परे सूचना का कोई अंतरोधन या मानीटर या विगूढ़न करने की अपेक्षा करता है तो, यथास्थिति, उस राज्य या संघ राज्य क्षेत्र में गृह विभाग का भारसाधक सचिव सूचना का ऐसा अंतरोधन या मानीटर या विगूढ़न करने के लिए समुचित प्राधिकारी को निदेश जारी करने के लिए, भारत सरकार के गृह मंत्रालय के सचिव से अनुरोध करेगा ।

7. निदेश की अंतर्वस्तुएं.— नियम 3 के अधीन सक्षम प्राधिकारी द्वारा जारी किए गए किसी निदेश में ऐसे निदेश के लिए कारण अंतर्विष्ट होंगे और ऐसे निदेश की एक प्रति सात कार्य दिवसों की अवधि के भीतर पुनर्विलोकन समिति को भेजी जाएगी ।

8. सक्षम प्राधिकारी द्वारा सूचना का अर्जन करने में वैकल्पिक साधनों पर विचार किया जाना.— सक्षम प्राधिकारी, नियम 3 के अधीन कोई निदेश जारी करने से पूर्व अन्य साधनों द्वारा आवश्यक सूचना अर्जित करने की संभावना पर विचार करेगा और नियम 3 के अधीन निदेश केवल तब जारी किया जाएगा जब अन्य युक्तियुक्त साधन द्वारा सूचना अर्जित करना संभव न हो ।

9. किसी विनिर्दिष्ट सूचना के अंतरोधन या मानीटर या विगूढ़न करने के लिए निदेश— किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त या भंडारित किसी सूचना के अंतरोधन या मानीटर या विगूढ़न करने का निदेश किसी ऐसी सूचना के बारे में होगा जो किसी व्यक्ति या किसी वर्ग के व्यक्तियों को या उसे भेजी जाती है या किसी विशिष्ट विषय से संबंधित है, चाहे ऐसी सूचना या वर्ग की सूचना एक या अधिक कंप्यूटर साधनों या ऐसे कंप्यूटर साधन में प्राप्त की जाती है जिसका एक विशिष्ट व्यक्ति से या को या एक या अधिक सेट के परिसरों लिए, जो निदेश में विनिर्दिष्ट या वर्णित किए जाएं, सूचना के जनन, पारेषण, प्राप्त करने, भंडार करने के लिए उपयोग किए जाने की संभावना है ।

10. उस अधिकारी का, जिसको सूचना प्रकट की जानी है, नाम और पदाभिधान विनिर्दिष्ट करने के लिए निदेश.— नियम 3 के अधीन प्रत्येक निदेश में उस प्राधिकृत अभिकरण के अधिकारी का नाम और पदाभिधान विनिर्दिष्ट होगा, जिसको अंतरुद्ध या मानीटर या विगूढ़ित की गई या भंडारित सूचना प्रकट की जाएगी, और यह भी विनिर्दिष्ट होगा कि अंतरुद्ध या मानीटर या विगूढ़ित की गई सूचना का उपयोग उक्त अधिनियम की धारा 69 की उपधारा (1) के उपबंधों के अधीन रहते हुए होगा ।

11. वह अवधि, जिसके भीतर निदेश प्रवृत्त रहेगा.— अंतरुद्ध या मानीटर या विगूढ़न करने के लिए निदेश, जब तक पहले प्रतिसंहृत नहीं कर दिया गया हो उसके जारी किए जाने की तारीख से 60 दिन से अनधिक की अवधि के लिए प्रवृत्त रहेगा और समय-समय पर एक सौ अस्सी दिन से अनधिक की अवधि के लिए नवीकृत किया जा सकेगा ।

12. नोडल अधिकारी को पदाभिहित करने के लिए प्राधिकृत अभिकरण.— नियम 4 के अधीन सक्षम प्राधिकारी द्वारा प्राधिकृत अभिकरण, एक या अधिक ऐसे नोडल अधिकारियों को, जो पुलिस अधीक्षक या अपर पुलिस अधीक्षक की पंक्ति से नीचे की पंक्ति न हो या समतुल्य पंक्ति के अधिकारी को, अधिप्रमाणित करने के लिए और अंतरोधन या मानीटर या विगूढ़न करने के लिए नियम 3 के अधीन जारी किए गए निदेश को पहुंचाने वाली अध्यपेक्षा को संबंधित मध्यवर्तियों के पदाभिहित अधिकारियों या कंप्यूटर साधन के भारसाधक व्यक्ति को भेजने के लिए पदाभिहित करेगा ।

परंतु कोई अधिकारी, जो पुलिस निरीक्षक की पंक्ति से नीचे की पंक्ति का न हो या समतुल्य पंक्ति का अधिकारी, मध्यवर्ती के पदाभिहित अधिकारी को परिदत्त परिदान करेगा ।

13. मध्यवर्ती द्वारा सुविधाएं आदि प्रदान किया जाना.— (1) सूचना का अंतरोधन या मानीटर या विगूढ़न करने के लिए नियम 3 के अधीन जारी किए गए निदेश को पहुंचाने वाली अध्यपेक्षा जारी करने वाला अधिकारी, मध्यवर्ती के पदाभिहित अधिकारियों या कंप्यूटर साधनों के भारसाधक व्यक्ति से निदेशों में वर्णित अंतरोधन या मानीटर या विगूढ़न करने के लिए सभी सुविधाएं, सहयोग और सहायता प्रदान करने के लिए लिखित रूप में भी अनुरोध करेगा ।

(2) उपनियम 1 के अधीन अनुरोध की प्राप्ति पर मध्यवर्ती के पदाभिहित अधिकारी या कंप्यूटर साधनों का भारसाधक व्यक्ति निदेश में वर्णित सूचना का अंतरोधन या मानीटर या उसके विगूढ़न करने के लिए सभी सुविधाएं, सहयोग और सहायता प्रदान करेंगे ।

(3) मध्यवर्ती को नियम 3 के अधीन जारी की गई सूचना के विगूढ़न का कोई निदेश उस विस्तार तक सीमित होगा, जिस तक सूचना मध्यवर्ती द्वारा गूढ़ की गई है या मध्यवर्ती विगूढ़ित कुंजी पर नियंत्रण रखता है ।

14. मध्यवर्ती द्वारा अध्यपेक्षा को प्राप्त करने और उस पर कार्रवाई करने के लिए अधिकारियों को पदाभिहित किया जाना.– प्रत्येक मध्यवर्ती या कंप्यूटर साधन का भारसाधक व्यक्ति किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त या भंडारित की गई सूचना का अंतर्रोधन या मानीटर या विगूढ़न करने हेतु नोडल अधिकारी से अध्यपेक्षा प्राप्त करने के लिए एक अधिकारी को और ऐसी अध्यपेक्षा पर कार्रवाई करने के लिए दूसरे अधिकारी को पदाभिहित करेगा ।

15. अनुदेश की अभिस्वीकृति.– मध्यवर्ती का पदाभिहित अधिकारी या कंप्यूटर साधनों का भारसाधक व्यक्ति, पत्रों या फैक्स द्वारा या इलेक्ट्रोनिक हस्ताक्षर से हस्ताक्षरित ई-मेल द्वारा उसे प्राप्त अनुदेशों की, सूचना के अंतर्रोधन या मानीटर या विगूढ़न के लिए ऐसी सूचना या निदेश की प्राप्ति के दो घंटों के भीतर, संबंधित अभिकरण के नोडल अधिकारी को अभिस्वीकृति देगा ।

16. पदाभिहित अधिकारी द्वारा अभिलेखों को रखा जाना.– किसी सूचना का अंतर्रोधन या मानीटर या विगूढ़न करने के लिए प्राधिकृत मध्यवर्ती का पदाभिहित अधिकारी या कंप्यूटर साधनों का भारसाधक व्यक्ति उचित अभिलेख रखेगा, जिनमें अंतर्रुद्ध या मानीटर या विगूढ़न की गई सूचना, व्यक्तियों की विशिष्टियां, कंप्यूटर साधन, ई-मेल लेखा, वेबसाइट पता आदि, जिसकी सूचना अंतर्रुद्ध या मानीटर या विगूढ़ित की गई है, उस अधिकारी या प्राधिकारी का नाम और अन्य विशिष्टियां जिसको अंतर्रुद्ध या मानीटर या विगूढ़ित की गई सूचना प्रकट की गई है, प्रतियों की संख्या, जिनके अंतर्गत, अंतर्रुद्ध या मानीटर या विगूढ़ित की गई सूचना के तत्संबंधी इलेक्ट्रोनिक अभिलेख और वह तरीका या पद्धति, जिसके द्वारा ऐसी प्रतियां, तत्संबंधी इलेक्ट्रोनिक अभिलेख सहित, बनाई जाती हैं, प्रतियों के तत्संबंधी इलेक्ट्रोनिक अभिलेखों सहित, नष्ट करने की तारीख और वह अवधि, जिसके भीतर निदेश प्रवृत्त रहते हैं, वर्णित होगी ।

17. विगूढ़न कुंजी को प्रकट करने या विगूढ़न सहायता प्रदान करने के लिए विगूढ़न कुंजीधारक.– यदि कोई विगूढ़न निदेश या उसकी कोई प्रति उस विगूढ़न कुंजीधारक को सौंपी जाती है, जिसको नियम 12 में निर्दिष्ट नोडल अधिकारी द्वारा विगूढ़न निदेश संबोधित किया गया है, तो विगूढ़न कुंजीधारक विगूढ़न निदेश में वर्णित अवधि के भीतर संबंधित प्राधिकारी व्यक्ति को विगूढ़न निदेश में विनिर्दिष्ट की गई –

(क) विगूढ़न कुंजी प्रकट करेगा ; या

(ख) विगूढ़न सहायता प्रदान करेगा ।

18. सूचना को अंतर्रुद्ध या मानीटर या विगूढ़न करने की सूची का प्रस्तुत किया जाना–(1) मध्यवर्ती के पदाभिहित अधिकारी या कंप्यूटर साधनों का भारसाधक व्यक्ति प्रत्येक पंद्रह दिन में पूर्ववर्ती पक्ष के दौरान उसके द्वारा प्राप्त किए गए अंतर्रोधन या मानीटरिंग या विगूढ़न प्राधिकारों की सूची, ऐसे प्राधिकारों की प्राधिकारिता की पुष्टि के लिए नियम 4 के अधीन प्राधिकृत अभिकरणों के नोडल अधिकारियों को अग्रेषित करेगा ।

(2) उपनियम (1) में निर्दिष्ट सूची में ऐसे ब्यौरे सम्मिलित होंगे, जैसे कि संबंधित सक्षम प्राधिकारी के आदेशों का निर्देश और तारीख, जिनके अंतर्गत आपात दशाओं के अधीन जारी किया गया कोई आदेश है, ऐसे आदेश की प्राप्ति की तारीख और समय और ऐसे आदेश के कार्यान्वयन की तारीख और समय ।

19. मध्यवर्ती द्वारा सूचना का अंतर्रोधन या मानीटर या विगूढ़न करने के मामले में कार्रवाई करने में प्रभावी नियंत्रण सुनिश्चित किया जाना–नियम 3 के अधीन इस प्रकार निदेशित किया गया मध्यवर्ती या कंप्यूटर साधन का भारसाधक व्यक्ति अंतर्रोधन या मानीटर या विगूढ़न करने के लिए, जिनमें निम्नलिखित प्रयोजनों के लिए भी सम्मिलित हैं,-

(i) नोडल अधिकारी द्वारा दिए गए निदेशों के अनुसार भंडारित सूचना में अंतर्रोधन या मानीटर या विगूढ़न करने या उस तक पहुंच प्राप्त करने के लिए नियम 4 के अधीन प्राधिकृत अभिकरण के उपकरण का संस्थापन ; या

(ii) ऐसे उपकरण का अनुरक्षण, परीक्षण या उपयोग ; या

(iii) ऐसे उपकरण का हटाना ; या

(iv) नियम 3 के अधीन सक्षम प्राधिकारी द्वारा जारी किए गए निदेश के अधीन भंडारित सूचना तक पहुंच प्राप्त करने के लिए अपेक्षित किसी कार्रवाई का निष्पादन ;

जब कभी नियम 4 के अधीन प्राधिकृत अभिकरण द्वारा अनुरोध किया जाए, तकनीकी सहायता और उपस्कर, जिनके अंतर्गत हार्डवेयर सॉफ्टवेयर, फर्मवेयर, भंडारण, अंतरापृष्ठ और उपकरण तक पहुंच है, प्रदान करेगा ।

20. मध्यवर्ती द्वारा सूचना का अंतरोधन या मानीटर या विगूढ़न करने के मामले में कार्रवाई करने में प्रभावी नियंत्रण सुनिश्चित किया जाना–मध्यवर्ती या कंप्यूटर साधनों का भारसाधक व्यक्ति यह सुनिश्चित करने के लिए कि सूचना में अप्राधिकृत व्यवधान नहीं डाला जाता है और अत्यधिक गोपनीयता बनाई रखी जाती है, उस स्थान में पर्याप्त और प्रभावी आंतरिक नियंत्रण रखेगा और सूचना में व्यवधान डालने या उसका मानीटर करने या विगूढ़न के मामले में अत्यधिक सतर्कता और पूर्वावधानी रखी जाएगी, क्योंकि इससे नागारिकों की एकांतता पर प्रभाव पड़ता है और उस पर मध्यवर्ती के पदाभिहित अधिकारियों द्वारा ही कार्रवाई की जाती है तथा मध्यवर्ती या कंप्यूटर साधन को भारसाधक व्यक्ति के किसी अन्य व्यक्ति की ऐसी अंतरोधित, मानीटर या विगूढ़ित सूचना तक पहुंच नहीं होगी ।

21. मध्यवर्ती का उत्तरदायित्व–मध्यवर्ती या कंप्यूटर साधनों का भारसाधक व्यक्ति अपने कर्मचारियों के किसी कार्य के लिए भी उत्तरदायी होगा और सूचना की गोपनीयता और विश्वसनीयता के अनुरक्षण से संबंधित उल्लंघन की दशा में या सूचना का कोई अप्राधिकृत अंतरोधन या मानीटर या विगूढ़न करने की दशा में मध्यवर्ती या कंप्यूटर साधनों का भारसाधक व्यक्ति तत्समय प्रवृत्त विधियों के सुसंगत उपबंधों के अधीन किसी कार्रवाई के लिए दायी होगा ।

22. सक्षम प्राधिकारी के निदेशों का पुनर्विलोकन–पुनर्विलोकन समिति की बैठक दो मास में कम से कम एक बार होगी और वह अपने ऐसे निष्कर्षों को कि क्या नियम 3 के अधीन जारी किए गए निदेश अधिनियम की धारा 69 की उपधारा (2) के उपबंधों के अनुसार हैं, अभिलिखित करेगी और जहां पुनर्विलोकन समिति की यह राय है कि निदेश ऊपर निर्दिष्ट उपबंधों के अनुसार नहीं है वहां वह निदेशों को अपास्त कर सकेगी और ऐसी प्रतियों को, जिनके अंतर्गत अंतरुद्ध मानीटर या विगूढ़ित की गई सूचना के तत्संबंधी इलेक्ट्रोनिक अभिलेख हैं, नष्ट करने के लिए आदेश जारी कर सकेगी ।

23. सूचना का अंतरोधन या मानीटर या विगूढ़न करने के अभिलेखों का नष्ट किया जाना–(1) प्रत्येक अभिलेख, जिसके अंतर्गत सूचना का अंतरोधन या मानीटर या विगूढ़न करने के लिए ऐसे निदेशों से और अंतरुद्ध या मानीटर या विगूढ़ित की गई सूचना से संबंधित इलेक्ट्रोनिक अभिलेख भी हैं, प्रत्येक छह मास में सुरक्षा अभिकरण द्वारा, सिवाए उस दशा के जहां ऐसी सूचना कृत्यकारी अपेक्षाओं के लिए अपेक्षित है या अपेक्षित होने की संभावना है, नष्ट कर दी जाएगी ।

(2) किसी चल रहे अन्वेषण, आपराधिक परिवाद या विधिक कार्यवाहियों के प्रयोजन के लिए अपेक्षित से अन्यथा के सिवाए, मध्यवर्ती या कंप्यूटर साधनों का भारसाधक व्यक्ति ऐसी सूचना का अंतरोधन या मानीटर या विगूढ़न करना बंद किए जाने के दो वर्ष की अवधि के भीतर सूचना के अंतरोधन के लिए निदेशों से संबंधित अभिलेखों को नष्ट करेगा और ऐसा करने में वे अत्यधिक गोपनीयता रखेंगे ।

24. प्राधिकरण के बिना सूचना का अंतरोधन या मानीटर या विगूढ़न करने का प्रतिषेध–(1) कोई व्यक्ति, जो साशय या जानबूझकर, नियम 3 या 4 के अधीन प्राधिकार के बिना किसी सूचना को भारत के भीतर किसी स्थान पर उसके होने या उसके पारेषण के अनुक्रम में अंतरुद्ध करता है, या करने का प्रयास करता है या किसी दूसरे व्यक्ति की अंतरुद्ध करने में या अंतरुद्ध करने का प्रयास करने में सहायता करता है, उसके विरुद्ध कार्यवाही की जाएगी और तत्समय प्रवृत्त विधियों के सुसंगत उपबंधों के अधीन तदनुसार उसे दंडित किया जाएगा ।

(2) किसी मध्यवर्ती के कर्मचारी या कंप्यूटर साधन के भारसाधक व्यक्ति द्वारा या मध्यवर्ती द्वारा सम्यक रूप से प्राधिकृत किसी व्यक्ति द्वारा कंप्यूटर साधन में सूचना के किसी अंतरोधन, मानीटर या विगूढ़न करने को उस मध्यवर्ती द्वारा प्रदाय की गई सेवाओं से संबंधित उसके कर्तव्य के अनुक्रम में लिया जाएगा, यदि ऐसे कार्यकलाप प्रचलित उद्योग पद्धतियों के अनुसार उसके कर्तव्यों के निर्वहन के लिए निम्नलिखित मामलों के संबंध में युक्तियुक्त रूप से आवश्यक हैं :-

(i) कंप्यूटर साधन या कंप्यूटर साधन के साथ प्रयोग किए जाने वाले किसी उपस्कर का संस्थापन ;

(ii) कंप्यूटर साधन का प्रचालन या अनुरक्षण ; या

(iii) मध्यवर्ती अथवा अभिदाता के लिए किसी संचार लिंक या सॉफ्टवेयर का संस्थापन या मध्यवर्ती के कंप्यूटर साधन पर उपयोगकर्ता के लेखा का संस्थापन और उसकी कृत्यकारिता के लिए उसका परीक्षण ;

(iv) उपस्कर, कंप्यूटर साधन या किसी संचार लिंक या कोड के संस्थापन, संयोजन या अनुरक्षण से संबंधित कंप्यूटर साधन से भंडारित सूचना तक पहुंचना ; या

(v) कंप्यूटर साधन से निम्नलिखित प्रयोजन के लिए भंडारित सूचना तक पहुंचना :

(क) कंप्यूटर साधन में सूचना सुरक्षा पद्धतियों को कार्यान्वित करना ;

(ख) सुरक्षा भंगों, कंप्यूटर संदूषकों या कंप्यूटर वायरस का अवधारण करना ;

(ग) अन्वेषण या आंतरिक संपरीक्षा के भाग रूप में संबंधित कंप्यूटर साधन के फॉरेंसिक कार्य का उत्तरदायित्व लेना ; या

(vi) कंप्यूटर साधन या ऐसे किसी व्यक्ति का, जिसने अधिनियम के किसी उपबंध का उल्लंघन किया है या जिसके बारे में उल्लंघन करने का संदेह है या जिसके उल्लंघन करने की संभावना है, जिससे मध्यवर्ती द्वारा प्रदाय की गई सेवाओं पर प्रतिकूल प्रभाव पड़ने की संभावना है, खोज करने के प्रयोजन के लिए कंप्यूटर साधन से सूचना तक पहुंच प्राप्त करना या उसका विश्लेषण करना ।

(3) मध्यवर्ती या कंप्यूटर साधन का भारसाधक व्यक्ति और उसके कर्मचारी उपनियम (2) के अधीन विनिर्दिष्ट कार्यों का पालन करते हुए सूचना की कड़ी गोपनीयता और विश्वसनीयता का अनुरक्षण करेंगे ।

25. अंतर्रुद्ध या मानीटर या विगूढ़ित की गई सूचना को प्रकट करने का प्रतिषेध-- (1) अंतर्रुद्ध या मानीटर की गई या भंडारित या विगूढ़ित सूचना की अंतर्वस्तुओं का मध्यवर्ती या उसके किसी कर्मचारी द्वारा या कंप्यूटर साधन के भारसाधक व्यक्ति द्वारा उपयोग नहीं किया जाएगा या उसे नियम 10 के अधीन उक्त सूचना के आशयित प्राप्तकर्ता से भिन्न किसी व्यक्ति को प्रकट नहीं किया जाएगा ।

(2) अंतर्रुद्ध या मानीटर या विगूढ़ित की गई सूचना की अंतर्वस्तुओं को नियम 4 के अधीन प्राधिकृत अभिकरण द्वारा किसी अन्य प्रयोजन के लिए, अन्वेषण के प्रयोजन के लिए या भारत में सक्षम न्यायालय के समक्ष न्यायिक कार्यवाहियों में अन्य सुरक्षा अभिकरण के साथ भागीदारी के लिए, प्रकट नहीं किया जाएगा ।

(3) उपनियम (2) में यथा अन्यथा उपबंधित के सिवाए अंतर्रुद्ध या मानीटर या विगूढ़ित की गई सूचना की अंतर्वस्तुओं को भारत में सक्षम न्यायालय के पूर्व आदेश के बिना, सार्वजनिक रूप से किन्हीं साधनों द्वारा प्रकट नहीं किया जाएगा या उसकी रिपोर्ट नहीं की जाएगी ।

(4) उपनियम (2) में यथा अन्यथा उपबंधित के सिवाय संबंधित सक्षम प्राधिकारी या नोडल अधिकारियों द्वारा अंतर्रुद्ध, मानीटर या विगूढ़न करने के लिए जारी किए गए निदेश के संबंध में कड़ी गोपनीयता रखी जाएगी ।

(5) ऐसे किसी मध्यवर्ती या उसके कर्मचारी या कंप्यूटर साधन के भारसाधक व्यक्ति के विरुद्ध, जो इन नियमों के उपबंधों का उल्लंघन करता है, कार्यवाही की जाएगी और उन्हें तत्समय प्रवृत्त अधिनियम के सुसंगत उपबंधों के अधीन तदनुसार दंडित किया जाएगा ।

(6) जब कभी केंद्र के संबंधित सुरक्षा अभिकरण द्वारा मांग की जाए तो राज्य और संघ राज्य क्षेत्र स्तर पर सुरक्षा अभिकरण तुरंत किसी सूचना को, जो उन्होंने नियम 3 के अधीन किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त या भंडारित किसी सूचना का अंतर्रोधन या मानीटर या विगूढ़न करने के लिए निदेशों के अनुसरण में प्राप्त की हो, तत्परता से बांटेंगे ।

[सं. 9(16)/2004 ई.सी.]

एन. रवि शंकर, संयुक्त सचिव

NOTIFICATION

New Delhi, the 27th October, 2009

G.S.R. 780 (E).— 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 (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 Safeguards 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 (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 –

(i) the Secretary in the Ministry of Home Affairs, in case of the Central Government; or

(ii) the Secretary in charge of the Home Department, in case of a State Government or Union territory, as the case may be;

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

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

(g) "decryption assistance" means any assistance to –

(i) allow access, to the extent possible, to encrypted information; or

(ii) facilitate conversion of encrypted information into an intelligible form;

(h) "decryption direction" means a direction issued under rule 3 in which a decryption key holder is directed to –

(i) disclose a decryption key; or

(ii) provide decryption assistance in respect of encrypted information

(i) "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;

(j) "decryption key holder" means any person who deploys the decryption mechanism and who is in possession of a decryption key for purposes of subsequent decryption of encrypted information relating to direct or indirect communications;

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

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

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

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

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

(m) "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 information; and any reference to an "interception device" includes, where applicable, a reference to a "monitoring device";

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

(o) "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;

(p) "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;

(q) "Review Committee" means the Review Committee constituted under rule 419A of Indian Telegraph Rules, 1951.

3. **Directions for interception or monitoring or decryption of any information.**— No person shall carry out the 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 Act, except by an order issued by the competent authority:

Provided that in an unavoidable circumstances, such order may be issued by an officer, not below the rank of the Joint Secretary to the Government of India, who has been duly authorised by the competent authority:

Provided further that in a case of emergency–

(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 interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource may be carried out with the prior approval of the Head or the second senior most officer of the security and law enforcement agency (hereinafter referred to as the said security agency) at the Central level and the officer authorised in this behalf, not below the rank of the Inspector General of Police or an officer of equivalent rank, at the State or Union territory level:

Provided also that the officer, who approved such interception or monitoring or decryption of information in case of emergency, shall inform in writing to the competent authority about the emergency and of such interception or monitoring or decryption within three working days and obtain the approval of the competent authority thereon within a period of seven working days and if the approval of competent authority is not obtained within the said period of seven working days, such interception or monitoring or decryption shall cease and the information shall not be intercepted or monitored or decrypted thereafter without the prior approval of the competent authority.

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

5. **Issue of decryption direction by competent authority.**— The competent authority may, under rule 3 give any decryption direction to the decryption key holder for decryption of any information involving a computer resource or part thereof.

6. **Interception or monitoring or decryption of information by a State beyond its jurisdiction.**— Notwithstanding anything contained in rule 3, if a State Government or Union territory Administration requires any interception or monitoring or decryption of information beyond its territorial jurisdiction, the Secretary in-charge of the Home Department in that State or Union territory, as the case may be, shall make a request to the Secretary in the Ministry of Home Affairs, Government of India for issuing direction to the appropriate authority for such interception or monitoring or decryption of information.

7. **Contents of direction.**— Any direction issued by the 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. **Competent authority to consider alternative means in acquiring information.**— The competent authority shall, before issuing any direction under rule 3, consider possibility of acquiring the necessary information by other means and the direction under rule 3 shall be issued only when it is not possible to acquire the information by any other reasonable means.

9. **Direction of interception or monitoring or decryption of any specific information.**— The direction of interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource shall be 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, or being a computer resource likely to be used for the generation, transmission, receiving, storing of information from or to one particular person or one or many set of premises, as may be specified or described in the direction.

10. **Direction to specify the name and designation of the officer to whom information to be disclosed.**— Every directions under rule 3 shall specify the name and designation of the officer of the authorised agency to whom the intercepted or monitored or decrypted or stored information shall be disclosed and also specify that the use of intercepted or monitored or decrypted information shall be subject to the provisions of sub-section (1) of section 69 of the said Act.

11. **Period within which direction shall remain in force**.— The direction for interception or monitoring or decryption shall remain in force, unless revoked earlier, for a period not exceeding sixty days from the date of its issue and may be renewed from time to time for such period not exceeding the total period of one hundred and eighty days.

12. **Authorised agency to designate nodal officer.**— The agency authorised by the competent authority under rule 4 shall designate one or more nodal officer, 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 requisition 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:

Provided that an officer, not below the rank of Inspector of Police or officer of equivalent rank, shall deliver the requisition to the designated officer of the intermediary.

13. **Intermediary to provide facilities, etc.**— (1) The officer issuing the requisition conveying direction issued under rule 3 for interception or monitoring or decryption of information shall also make a request in writing to the designated officers of intermediary or person in-charge of computer resources, to provide all facilities, co-operation and assistance for interception or monitoring or decryption mentioned in the directions.

(2) On the receipt of request under sub-rule (1), the designated officers of intermediary or person in-charge of computer resources, shall provide all facilities, co-operation and assistance for interception or monitoring or decryption of information mentioned in the direction.

(3) Any direction of decryption of information issued under rule 3 to intermediary shall be limited to the extent the information is encrypted by the intermediary or the intermediary has control over the decryption key.

14. **Intermediary to designate officers to receive and handle requisition.**— Every intermediary or person in-charge of computer resource shall designate an officer to receive requisition, and another officer 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. **Acknowledgement of instruction.**— The designated officer of the intermediary or person in-charge of computer resources shall acknowledge the instructions received by him through letters or fax or e-mail signed with electronic signature to the nodal officer of the concerned agency within two hours on receipt of such intimation or direction for interception or monitoring or decryption of information.

16. **Maintenance of records by designated officer.**— 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, e-mail account, 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. **Decryption key holder to disclose decryption key or provide decryption assistance.**— 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 referred to in rule 12, the decryption key holder shall within the period mentioned in the decryption direction –

(a) disclose the decryption key; or

(b) provide the decryption assistance,

specified in the decryption direction to the concerned authorised person.

18. **Submission of list of interception or monitoring or decryption of information.**— (1) The designated officers of the intermediary or person in-charge of computer resources shall forward in every fifteen days a list of interception or monitoring or decryption authorisations received by them during the preceding fortnight to the nodal officers of the agencies authorised under rule 4 for confirmation of the authenticity of such authorisations.

(2) The list referred to in sub-rule (1) shall include details, such as the reference and date of orders of the concerned competent authority including any order issued under emergency cases, date and time of receipt of such order and the date and time of implementation of such order.

19. **Intermediary to ensure effective check in handling matter of interception or monitoring or decryption of information.**— The intermediary or the person in-charge of the computer resource so directed under rule 3, shall provide technical assistance and the equipment including hardware, software, firmware, storage, interface and access to the equipment wherever requested by the agency authorised under rule 4 for performing interception or monitoring or decryption including for the purposes of-

(i) the installation of equipment of the agency authorised under rule 4 for the purposes of interception or monitoring or decryption or accessing stored information in accordance with directions by the nodal officer; or

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

(iii) the removal of such equipment; or

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

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

21. **Responsibility of intermediary.**— The intermediary or person in-charge of computer resources shall be responsible for any action of their employees also and in case of violation pertaining to maintenance of secrecy and confidentiality of information or any unauthorised interception or monitoring or decryption of information, the intermediary or person in-charge of computer resources shall be liable for any action under the relevant provisions of the laws for the time being in force..

22. **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 rule 3 are in accordance with the provisions of sub-section (2) of section 69 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 intercepted or monitored or decrypted information.

23. **Destruction of records of interception or monitoring or decryption of information.**— (1) Every record, 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 security agency in every six months except in a case where such information is required, 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 person in-charge of computer resources shall destroy records pertaining to directions for interception of information within a period of two months of discontinuance of the interception or monitoring or decryption of such information and in doing so they shall maintain extreme secrecy.

24. **Prohibition of interception or monitoring or decryption of information without authorisation.**— (1) Any person who intentionally or knowingly, without authorisation under rule 3 or 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 and punished accordingly under the relevant provisions of the laws for the time being in force.

(2) 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, 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 specified under sub-rule (2).

25. **Prohibition of disclosure of intercepted or monitored or decrypted information.**— (1) 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.

(2) The contents of intercepted or monitored or decrypted information shall not be used or disclosed by the agency authorised under rule 4 for any other purpose, except for investigation or sharing with other security agency for the purpose of investigation or in judicial proceedings before the competent court in India.

(3) Save as otherwise provided in sub-rule (2), the contents of intercepted or monitored or decrypted information shall not be disclosed or reported in public by any means, without the prior order of the competent court in India.

(4) Save as otherwise provided in sub-rule (2), strict confidentiality shall be maintained in respect of direction for interception, monitoring or decryption issued by concerned competent authority or the nodal officers.

(5) Any intermediary or its employees or person in-charge of computer resource who contravenes provisions of these rules shall be proceeded against and punished accordingly under the relevant provisions of the Act for the time being in force.

(6) Whenever asked for by the concerned security agency at the Centre, the security agencies at the State and the Union territory level shall promptly share any information which they 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 agency at the Centre.

[No. 9(16)/2004-EC]
N. RAVI SHANKER, Jt. Secy.

अधिसूचना

नई दिल्ली, 27 अक्तूबर, 2009

सा.का.नि. 781(अ).— . केंद्रीय सरकार, केंद्रीय सूचना प्रौद्योगिकी अधिनियम, 2000, (2000 का 21) की धारा 69क की उपधारा (2) के साथ पठित, धारा 87 की उपधारा (2) के खंड (य) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए निम्नलिखित नियम बनाती है, अर्थात, :

1. **संक्षिप्त नाम और प्रारंभ** – (1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (सूचना को जनता की पहुंच के लिए अवरुध करने की प्रक्रिया और रक्षोपाय) नियम, 2009 है ।

(2) ये राजपत्र में प्रकाशन की तारीख को प्रवृत्त होंगे ।

2. **परिभाषाएं.** – इन नियमों में, जब तक कि संदर्भ से अन्यथा अपेक्षित न हों :-

(क) "अधिनियम" से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है ;

(ख) "कंप्यूटर साधन" से अधिनियम की धारा 2 की उपधारा (1) के खंड (ट) में यथा परिभाषित कंप्यूटर साधन अभिप्रेत है ;

(ग) "पदाभिहित अधिकारी" से नियम 3 के अधीन पदाभिहित अधिकारी के रूप में पदाभिहित कोई अधिकारी अभिप्रेत है ;

(घ) "प्ररुप" से इन नियमों से संलग्न कोई प्ररुप अभिप्रेत है ;

(ङ) "मध्यवर्ती" से अधिनियम की धारा 2 की उपधारा (1) के खंड (ब) में यथा परिभाषित कोई मध्यवर्ती अभिप्रेत है ;

(च) "नोडल अधिकारी" से नियम 4 के अधीन उस रूप में पदाभिहित नोडल अधिकारी अभिप्रेत है ;

(छ) "संगठन" से निम्नलिखित अभिप्रेत है –

(i) भारत सरकार के मंत्रालय या विभाग ;

(ii) राज्य सरकार और संघ राज्य क्षेत्र ;

(iii) केंद्रीय सरकार का ऐसा कोई अभिकरण, जो केंद्रीय सरकार द्वारा राजपत्र में अधिसूचित किया जाए ;

(ज) "अनुरोध" से किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त, भंडारित या परपोषित किसी सूचना को जनता की पहुंच के लिए अवरुद्ध करने के लिए अनुरोध अभिप्रेत है ;

(झ) "पुनर्विलोकन समिति" से भारतीय तार अधिनियम, 1951 के नियम 419क के अधीन गठित पुनर्विलोकन समिति अभिप्रेत है ;

3. **पदाभिहित अधिकारी.**– केंद्रीय सरकार, राजपत्र में अधिसूचना द्वारा, केंद्रीय सरकार के किसी अधिकारी को, जो संयुक्त सचिव की पंक्ति से नीचे की पंक्ति का न हो, अधिनियम की धारा 69क की उपधारा (2) के अधीन

किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त, भंडारित या परपोषित किसी सूचना को जनता की पहुंच के लिए अवरुद्ध करने का निदेश जारी करने के प्रयोजनार्थ "पदाभिहित अधिकारी" के रूप में पदाभिहित करेगी ।

4. संगठन का नोडल अधिकारी.– प्रत्येक संगठन इन नियमों के प्रयोजन के लिए, अपने अधिकारियों में से किसी अधिकारी को नोडल अधिकारी के रूप में पदाभिहित करेगा और उसकी सूचना संचार और प्रौद्योगिकी मंत्रालय, भारत सरकार के अधीन सूचना प्रौद्योगिकी विभाग में केंद्रीय सरकार को देगा और उक्त नोडल अधिकारी का नाम अपने वेबसाइट पर भी प्रकाशित करेगा ।

5. पदाभिहित अधिकारी द्वारा निदेश.– पदाभिहित अधिकारी, किसी संगठन के नोडल अधिकारी या किसी सक्षम न्यायालय से किसी अनुरोध की प्राप्ति पर, आदेश द्वारा सरकार के किसी अभिकरण या मध्यवर्ती को अधिनियम की धारा 69क की उपधारा (2) में विनिर्दिष्ट कारणों में से किसी कारण से किसी कंप्यूर साधन में जनित पारेषित, प्राप्त, भंडारित या परपोषित किसी सूचना या उसके भाग को जनता की पहुंच के लिए अवरुद्ध करने के लिए निदेश दे सकेगा ।

6. संगठन द्वारा अनुरोध का भेजा जाना.– (1) कोई व्यक्ति संबंधित संगठन के नोडल अधिकारी को किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त, भंडारित या परपोषित किसी सूचना को जनता की पहुंच के लिए अवरुद्ध करने के लिए अपनी शिकायत भेज सकेगा :

परंतु कोई अनुरोध संगठन के नोडल अधिकारी से अन्यथा, संबंधित राज्य या संघ राज्य क्षेत्र के मुख्य सचिव के अनुमोदन से पदाभिहित अधिकारी को भेजा जाएगा :

परंतु यह और कि यदि किसी संघ राज्य क्षेत्र में कोई मुख्य सचिव नहीं है तो ऐसे अनुरोध का उस संघ राज्य क्षेत्र के प्रशासक के सलाहकार द्वारा अनुमोदन किया जा सकेगा ।

(2) संगठन उप-नियम (1) के अधीन प्राप्त किसी शिकायत की अधिनियम की, अधिनियम की धारा 69क की उपधारा (1) में प्रगणित कारणों के संबंध में कार्रवाई करने की आवश्यकता के बारे में में अपना समाधान करने के लिए परीक्षा करेगा और समाधान हो जाने के पश्चात् वह अनुरोध को अपने नोडल अधिकारी के माध्यम से इन नियमों से संलग्न प्ररूप में विनिर्दिष्ट रूप विधान में पदाभिहित अधिकारी को भेजेगा ।

(3) पदाभिहित अधिकारी किसी व्यक्ति से सूचना को अवरुद्ध करने के लिए किसी शिकायत या अनुरोध को सीधे ग्रहण नहीं करेगा ।

(4) अनुरोध संबंधित संगठन के शीर्षनामे पर लिखित रूप में सभी पहलुओं से पूर्ण होगा और डाक द्वारा या फैक्स द्वारा या नोडल अधिकारी के इलेक्ट्रोनिक चिह्नक से हस्ताक्षरित ई-मेल द्वारा भेजा जा सकेगा :

परंतु यदि अनुरोध फैक्स द्वारा या ई-मेल द्वारा भेजा जाता है, जिसे इलेक्ट्रोनिक हस्ताक्षर द्वारा हस्ताक्षरित नहीं किया गया है, तो नोडल अधिकारी अनुरोध की एक हस्ताक्षरित प्रति उपलब्ध कराएगा, जिससे कि वह पदाभिहित अधिकारी के पास ऐसे फैक्स या ई-मेल द्वारा अनुरोध की प्राप्ति के तीन दिन की अवधि के भीतर पहुंच जाए ।

(5) प्राप्ति पर प्रत्येक अनुरोध को, पदाभिहित अधिकारी द्वारा उसकी प्राप्ति की तारीख और समय के साथ एक संख्या समनुदेशित की जाएगी और वह नोडल अधिकारी को, उसकी प्राप्ति के 24 घंटों की अवधि के भीतर, उसकी प्राप्ति की अभिस्वीकृति देगा ।

7. अनुरोध की परीक्षा के लिए समिति.– अनुरोध की अभिकथित नियम विरुद्ध सूचना या उसके भाग की मुद्रित नमूना अंतर्वस्तु के साथ एक ऐसी समिति द्वारा परीक्षा की जाएगी, जो अध्यक्ष के रूप में पदाभिहित अधिकारी और ऐसे प्रतिनिधियों से, जो विधि और न्याय, गृह, सूचना और प्रसारण मंत्रालयों के संयुक्त सचिव की पंक्ति से निम्न के न हों, और अधिनियम की धारा 70ख की उपधारा (1) के अधीन नियुक्त भारतीय कंप्यूटर आपात मोचन दल से मिलकर बनेगी ।

8. अनुरोध की परीक्षा.– (1) नियम 6 के अधीन अनुरोध की प्राप्ति पर, पदाभिहित अधिकारी उस व्यक्ति या मध्यवर्ती की पहचान करने के सभी युक्तियुक्त प्रयास करेगा जिसने सूचना या उसके भाग को और साथ ही उस

कंप्यूटर साधन को, जिस पर ऐसी सूचना या उसका भाग परपोषित किया जा रहा है, परपोषित किया है और जहां वह ऐसे व्यक्ति या मध्यवर्ती और उस सूचना या उसके भाग की, जिसको जनता की पहुंच के लिए अवरुद्ध करने का अनुरोध किया गया है, पहचान करने में समर्थ है, वहां वह ऐसे कंप्यूटर साधन के नियंत्रण में ऐसे व्यक्ति या मध्यवर्ती को पत्रों या फैक्स या इलेक्ट्रोनिक चिह्नक से चिह्नित ई-मेल के रूप में एक सूचना, नियम 7 में निर्दिष्ट समिति के समक्ष विनिर्दिष्ट तारीख और समय पर, जो ऐसे व्यक्ति या मध्यवर्ती द्वारा ऐसी सूचना की प्राप्ति के समय से कम से कम 48 घंटे से कम का नहीं होगा, प्रस्तुत होने और अपना उत्तर और स्पष्टीकरण, यदि कोई हों, प्रस्तुत करने के लिए जारी करेगा ।

(2) ऐसे व्यक्ति या मध्यवर्ती के, जिस पर उप-नियम (1) के अधीन सूचना की तामील की गई है, ऐसी विनिर्दिष्ट तारीख और समय पर समिति के समक्ष उपस्थित न होने की दशा में, समिति नोडल अधिकारी से प्राप्त अनुरोध के संबंध में लिखित में विनिर्दिष्ट सिफारिश देगी, जो समिति के पास उपलब्ध सूचना पर आधारित होगी ।

(3) यदि ऐसा कोई व्यक्ति या मध्यवर्ती, जिस पर उप-नियम (1) के अधीन सूचना की तामील की गई है, विदेशी अस्तित्व या निगमित निकाय है, जैसा पदाभिहित अधिकारी द्वारा पता लगाया गया है, तो सूचना पत्रों या फैक्स या इलेक्ट्रोनिक चिह्नक से चिह्नित ई-मेल द्वारा ऐसे विदेशी अस्तित्व या निगमित निकाय को भेजी जाएगी और कोई ऐसा विदेशी अस्तित्व या निगमित निकाय ऐसी सूचना का उसमें विनिर्दिष्ट समय के भीतर उत्तर देगा, जिसमें असफल रहने पर वह समिति नोडल अधिकारी से प्राप्त अनुरोध के संबंध में लिखित में, विनिर्दिष्ट सिफारिश देगी, जो समिति के पास उपलब्ध सूचना पर आधारित होगी ।

(4) नियम 7 में निर्दिष्ट समिति अनुरोध और मुद्रित नमूना सूचना की परीक्षा करेगी और इस बात पर विचार करेगी कि क्या अनुरोध अधिनियम की धारा 69क की उपधारा (1) की परिधि के भीतर आता है और ऐसी सूचना या उसके भाग को अवरूद्ध करना न्यायोचित है और नोडल अधिकारी से प्राप्त अनुरोध के संबंध में लिखित में विनिर्दिष्ट सिफारिश देगी ।

(5) पदाभिहित अधिकारी नोडल अधिकारी द्वारा भेजे गए ब्यौरों के साथ सूचना को अवरूद्ध करने के अनुरोध के संबंध में समिति की सिफारिश को संचार और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार के अधीन सूचना प्रौद्योगिकी विभाग में सचिव को (जिसे इसमें इसके पश्चात् 'सचिव', सूचना प्रौद्योगिकी विभाग' कहा गया है) प्रस्तुत करेगा ।

(6) पदाभिहित अधिकारी सचिव, सूचना प्रौद्योगिकी विभाग द्वारा अनुरोध का अनुमोदन किए जाने पर, सरकार के किसी अभिकरण या मध्यवर्ती को उनके कंप्यूटर साधन में जनित, पारेषित, प्राप्त, भंडारित या परपोषित नियम विरुद्ध सूचना को अवरूद्ध करने के लिए निदेशित करेगा :

परंतु यदि, नोडल अधिकारी के अनुरोध का सचिव, सूचना प्रौद्योगिकी विभाग द्वारा अनुमोदन नहीं किया जाता है तो पदाभिहित अधिकारी उसकी सूचना ऐसे नोडल अधिकारी को देगा ।

9. आपात की दशाओं में सूचना का अवरूद्ध किया जाना.– (1) नियम 7 और नियम 8 में अंतर्विष्ट किसी बात के होते हुए भी, पदाभिहित अधिकारी आपात प्रकृति के किसी मामले में, जिसके लिए कोई विलंब स्वीकार्य नहीं है, अनुरोध और मुद्रित नमूना सूचना की परीक्षा करेगा और इस पर विचार करेगा कि क्या अनुरोध अधिनियम की धारा 69क की उपधारा (1) के क्षेत्र के भीतर आता है और यह आवश्यक या समीचीन और न्यायोचित है कि ऐसी सूचना या उसके भाग को अवरूद्ध किया जाए और अनुरोध को लिखित में विनिर्दिष्ट सिफारिशों सहित सचिव, सूचना प्रौद्योगिकी विभाग को भेजेगा ।

(2) आपात प्रकृति के किसी मामले में, सचिव, सूचना प्रौद्योगिकी विभाग, यदि उसका यह समाधान हो जाता है कि किसी सूचना या उसके भाग को किसी कंप्यूटर साधन द्वारा जनता की पहुंच के लिए अवरूद्ध करना आवश्यक या समीचीन और न्यायोचित है, तो वह कारण अभिलिखित करने के पश्चात्, अंतरिम उपाय के रूप में ऐसी सूचना या उसके भाग को परपोषित करने वाले ऐसे कंप्यूटर साधन के नियंत्रण में ऐसे पहचान किए गए या पहचान किए जाने योग्य व्यक्तियों या मध्यवर्ती को, उसको सुनवाई का कोई अवसर दिए बिना, ऐसे निदेश जारी करेगा, जो वह आवश्यक समझे ।

(3) पदाभिहित अधिकारी शीघ्रतम, किंतु उप-नियम (2) के अधीन निदेश जारी करने के 48 घंटों के अपश्चात, अनुरोध को नियम 7 में निर्दिष्ट समिति के समक्ष उसके विचारण और सिफारिश के लिए लाएगा ।

(4) समिति की सिफारिशों की प्राप्ति पर सचिव, सूचना प्रौद्योगिकी विभाग ऐसी अनुरोध के अनुमोदन के संबंध में अंतिम आदेश पारित करेगा और यदि अवरूद्ध करने के लिए अनुरोध का सचिव, सूचना प्रौद्योगिकी विभाग द्वारा अपने अंतिम आदेश में अनुमोदन नहीं किया जाता है तो उप-नियम (2) के अधीन जारी किए गए अंतरिम निदेश को उपसंहृत किया जाएगा और ऐसी सूचना के नियंत्रण में उस व्यक्ति या मध्यवर्ती को जनता की पहुंच के लिए सूचना को अवरूद्ध न करने के लिए निदेशित किया जाएगा ।

10. सूचना को अवरूद्ध करने के लिए न्यायालय के आदेश की प्रक्रिया.– किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त, भंडारित या परपोषित किसी सूचना या उसके भाग को अवरूद्ध करने के लिए भारत में किसी सक्षम न्यायालय से किसी आदेश की दशा में, पदाभिहित अधिकारी न्यायालय के आदेश की प्रमाणित प्रति की प्राप्ति पर तुरंत उसे सचिव, सूचना प्रौद्योगिकी विभाग को प्रस्तुत करेगा और न्यायालय द्वारा निदेशित रूप में कार्रवाई प्रारंभ करेगा ।

11. अनुरोध का शीघ्र निपटारा.– नोडल अधिकारी से प्राप्त अनुरोध पर शीघ्रता से विनिश्चय किया जाएगा, जो किसी भी दशा में अनुरोध की प्राप्ति की तारीख से 7 कार्य-दिनों से अधिक नहीं होगा ।

12. मध्यवर्ती द्वारा निदेश का अननुपालन किए जाने के लिए कार्रवाई.– यदि मध्यवर्ती नियम 9 के अधीन उसको जारी किए गए निदेश का अनुपालन करने में असफल रहता है तो पदाभिहित अधिकारी सचिव, सूचना प्रौद्योगिकी विभाग के पूर्व अनुमोदन से ऐसी समुचित कार्रवाई प्रारंभ करेगा, जो अधिनियम की धारा 69क की उपधारा (3) के उपबंधों का अनुपालन करने के लिए अपेक्षित हो ।

13. मध्यवर्ती द्वारा निदेशों को प्राप्त करने और उन पर कार्रवाई करने के लिए किसी व्यक्ति को पदाभिहित किया जाना– (1) प्रत्येक मध्यवर्ती कम से कम एक व्यक्ति को इन नियमों के अधीन किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त, भंडारित या परपोषित किसी सूचना को जनता की पहुंच के लिए अवरूद्ध करने के निदेशों को प्राप्त करने और उन पर कार्रवाई करने के लिए पदाभिहित करेगा ।

(2) मध्यवर्ती का पदाभिहित व्यक्ति निदेश की प्राप्ति पर दो घंटे के भीतर पदाभिहित अधिकारी को अभिस्वीकृति पत्र या फैक्स या इलेक्ट्रॉनिक चिह्नक से चिह्नित ई-मेल द्वारा निदेश की प्राप्ति की अभिस्वीकृति देगा ।

14. पुनर्विलोकन समिति की बैठक.– पुनर्विलोकन समिति की दो मास में कम से कम एक बार बैठक होगी और वह अपने इस निष्कर्षों को अभिलिखित करेगी कि क्या इन नियमों के अधीन जारी किए गए निदेश अधिनियम की धारा 69क की उपधारा (1) के उपबंधों के अनुसार हैं और यदि उसकी यह राय है कि निदेश ऊपर निर्दिष्ट उपबंधों के अनुसार नहीं है, तो वह निदेशों को अपास्त कर सकेगी और जनता की पहुंच के लिए किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त, भंडारित या परपोषित उक्त सूचना को अनवरूद्ध करने के लिए आदेश जारी कर सकेगी ।

15. पदाभिहित अधिकारी द्वारा अभिलेखों का अनुरक्षण.– पदाभिहित अधिकारी प्राप्त किए गए अनुरोध और उस पर की गई कार्रवाई का पूर्ण अभिलेख इलेक्ट्रॉनिक डाटा संचय में और किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त, भंडारित या परपोषित सूचना के जनता की पहुंच के लिए अवरूद्ध करने के मामलों के रजिस्टर में भी रखेगा ।

16. अनुरोधों और शिकायतों का गोपनीय होना.– प्राप्त किए गए सभी अनुरोधों और शिकायतों और उनके बारे में की गई कार्रवाइयों के संबंध में कड़ी गोपनियता रखी जाएगी ।

प्ररूप

[नियम 6(2) देखिए]

क. शिकायत

1. शिकायतकर्ता का नाम : ....

(वह व्यक्ति, जिसने मंत्रालय/विभाग/राज्य सरकार/नोडल अधिकारी को शिकायत भेजी है)

2. पता : ....

....

शहर : .... पिन कोड : ....

3. टेलीफोन : .... (एसटीडी कोड पहले लगाएं) 4. फैक्स (यदि कोई हो) ....

5. मोबाइल (यदि कोई हो) : ....

6. ई-मेल (यदि कोई हो) : ....

ख : वेबसाइट/कंप्यूटर साधन/मध्यवर्ती/वेबसाइट पर परपोषित नियम विरुद्ध सूचना के ब्यौरे

(कृपया जहां कहीं ज्ञात हो, ब्यौरे दें)

7. यूआरएल/ वेब पता : ....

8. आई पी पता : ....

9. हाइपरलिंक : ....

10. सर्वर/प्रोक्सी सर्वर पता : ....

11. मध्यवर्ती का नाम : ....

12. मध्यवर्ती का यूआरएल : ....

(कृपया नियम विरुद्ध सूचना का स्क्रीन शॉट/प्रिन्ट आउट संलग्न करें)

13. मध्यवर्ती का पता या अवस्थिति यदि मध्यवर्ती दूरसंचार सेवा प्रदाता, नेटवर्क सेवा प्रदाता, इंटरनेट सेवा प्रदाता, वेब हॉस्टिंग सेवा प्रदाता और साइबर कैफे या अन्य प्रकार का ऐसा मध्यवर्ती है, जिसके लिए सूचना मद सं. (7), (8) (9), (10), (11) और (12) में उपलब्ध नहीं है ।

....

....

ग. अवरुद्ध करने के लिए अनुरोध के ब्यौरे

14. मंत्रालय/राज्य सरकार की सिफारिश/टिप्पणियां : ....

....

15. वह स्तर, जिस पर टिप्पणियों/सिफारिश का अनुमोदन किया गया है

(कृपया पदाभिधान विनिर्दिष्ट करें) : ....

16. क्या शिकायत की मंत्रालय/राज्य सरकार में परीक्षा की गई है : हां/नहीं

17. यदि हां, तो वह निम्नलिखित कारणों में से किसके अंतर्गत आती है (कृपया चिह्नित करें)

(i) भारत की प्रभुता और अखंडता का हित

(ii) भारत की रक्षा

(iii) राज्य की सुरक्षा

(iv) विदेशी राज्यों के साथ मित्रतापूर्ण संबंध

(v) लोक व्यवस्था

(vi) उपर्युक्त से संबंधित किसी संज्ञेय अपराध के किए जाने में उद्दीपन को रोकने के लिए

घ. मंत्रालय/राज्य सरकार की सिफारिश और संबंधित संलग्नकों के साथ शिकायत अग्रेषित करने वाले नोडल अधिकारी के ब्यौरे

18. नोडल अधिकारी का नाम : ....

19. पदाभिधान : ....

20. संगठन : ....

21. पता : ....

....

शहर : .... पिन कोड : ....

22. टेलीफोन : .... (एसटीडी कोड पहले लगाएं)

23. फैक्स (यदि कोई हो) ....

24. मोबाइल (यदि कोई हो) : ....

25. ई-मेल (यदि कोई हो) : ....

ङ. कोई अन्य सूचना

च. संलग्नक : 1.

2.

3.

तारीख : स्थान : हस्ताक्षर

[सं. 9(16)/2004-ई.सी.]

एन. रवि शंकर, संयुक्त सचिव

NOTIFICATION

New Delhi, the 27th October, 2009

G.S.R. 781 (E).— In exercise of the powers conferred by clause (z) of sub-section (2) of section 87, read with sub-section (2) of section 69A 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 Safeguards for Blocking for Access of Information by Public) 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) "computer resource" means computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;

(c) "Designated Officer" means an officer designated as Designated Officer under rule 3;

(d) "Form" means a form appended to these rules;

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

(f) "nodal officer" means the nodal officer designated as such under rule 4;

(g) "organisation" means –

(i)Ministries or Departments of the Government of India;

(ii) state Governments and Union territories;

(iii) any agency of the Central Government, as may be notified in the Official Gazette, by the Central Government;

(h) "request" means the request for blocking of access by the public any information generated, transmitted, received, stored or hosted in any computer resource;

(i) "Review Committee" means the Review Committee constituted under rule 419A of Indian Telegraph Rules, 1951.

3. Designated Officer.— The Central Government shall designate by notification in Official Gazette, an officer of the Central Government not below the rank of a Joint Secretary, as the "Designated Officer", for the purpose of issuing direction for blocking for access by the public any information generated, transmitted, received, stored or hosted in any computer resource under sub-section (2) of section 69A of the Act.

4. Nodal officer of organisation.— Every organisation for the purpose of these rules, shall designate one of its officer as the Nodal Officer and shall intimate the same to the Central Government in the Department of Information Technology under the Ministry of Communications and Information Technology, Government of India and also publish the name of the said Nodal Officer on their website.

5. Direction by Designated Officer.— The Designated Officer may, on receipt of any request from the Nodal Officer of an organisation or a competent court, by order direct any Agency of the Government or intermediary to block for access by the public any information or part thereof generated, transmitted, received, stored or hosted in any computer resource for any of the reasons specified in sub-section (1) of section 69A of the Act.

6. Forwarding of request by organisation.— (1) Any person may send their complaint to the Nodal Officer of the concerned organisation for blocking of access by the public any information generated, transmitted, received, stored or hosted in any computer resource:

Provided that any request, other than the one from the Nodal Officer of the organisation, shall be sent with the approval of the Chief Secretary of the concerned State or Union territory to the Designated Officer:

Provided further that in case a Union territory has no Chief Secretary, then, such request may be approved by the Adviser to the Administrator of that Union territory.

(2) The organisation shall examine the complaint received under sub-rule (1) to satisfy themselves about the need for taking of action in relation to the reasons enumerated in sub-section (1) of section 69A of the Act and after being satisfied, it shall send the request through its Nodal Officer to the Designated Officer in the format specified in the Form appended to these rules.

(3) The Designated Officer shall not entertain any complaint or request for blocking of information directly from any person.

(4) The request shall be in writing on the letter head of the respective organisation, complete in all respects and may be sent either by mail or by fax or by e-mail signed with electronic signature of the Nodal Officer:

Provided that in case the request is sent by fax or by e-mail which is not signed with electronic signature, the Nodal Officer shall provide a signed copy of the request so as to reach the Designated Officer within a period of three days of receipt of the request by such fax or e-mail.

(5) On receipt, each request shall be assigned a number alongwith the date and time of its receipt by the Designated Officer and he shall acknowledge the receipt thereof to the Nodal Officer within a period of twenty four hours of its receipt.

7. **Committee for examination of request.—** The request alongwith the printed sample content of the alleged offending information or part thereof shall be examined by a committee consisting of the Designated Officer as its chairperson and representatives, not below the rank of Joint Secretary in Ministries of Law and Justice, Home Affairs, Information and Broadcasting and the Indian Computer Emergency Response Team appointed under sub-section (1) of section 70B of the Act.

8. **Examination of request.—** (1) On receipt of request under rule 6, the Designated Officer shall make all reasonable efforts to identify the person or intermediary who has hosted the information or part thereof as well as the computer resource on which such information or part thereof is being hosted and where he is able to identify such person or intermediary and the computer resource hosting the information or part thereof which have been requested to be blocked for public access, he shall issue a notice by way of letters or fax or e-mail signed with electronic signatures to such person or intermediary in control of such computer resource to appear and submit their reply and clarifications, if any, before the committee referred to in rule 7, at a specified date and time, which shall not be less than forty-eight hours from the time of receipt of such notice by such person or intermediary.

(2) In case of non-appearance of such person or intermediary, who has been served with the notice under sub-rule (1), before the committee on such specified date and time, the committee shall give specific recommendation in writing with respect to the request received from the Nodal Officer, based on the information available with the committee.

(3) In case, such a person or intermediary, who has been served with the notice under sub-rule (1), is a foreign entity or body corporate as identified by the Designated Officer, notice shall be sent by way of letters or fax or e-mail signed with electronic signatures to such foreign entity or body corporate and any such foreign entity or body corporate shall respond to such a notice within the time specified therein, failing which the committee shall give specific recommendation in writing with respect to the request received from the Nodal Officer, based on the information available with the committee.

(4) The committee referred to in rule 7 shall examine the request and printed sample information and consider whether the request is covered within the scope of sub-section (1) of section 69A of the Act and that it is justifiable to block such information or part thereof and shall give specific recommendation in writing with respect to the request received from the Nodal Officer.

(5) The designated Officer shall submit the recommendation of the committee, in respect of the request for blocking of information alongwith the details sent by the Nodal Officer, to the Secretary in the Department of Information Technology under the Ministry of Communications and Information

Technology, Government of India (hereinafter referred to as the "Secretary, Department of Information Technology").

(6) The Designated Officer, on approval of the request by the Secretary, Department of Information Technology, shall direct any agency of the Government or the intermediary to block the offending information generated, transmitted, received, stored or hosted in their computer resource for public access within the time limit specified in the direction:

Provided that in case the request of the Nodal Officer is not approved by the Secretary, Department of Information Technology, the Designated Officer shall convey the same to such Nodal Officer.

9. **Blocking of information in cases of emergency.**— (1) Notwithstanding anything contained in rules 7 and 8, the Designated Officer, in any case of emergency nature, for which no delay is acceptable, shall examine the request and printed sample information and consider whether the request is within the scope of sub-section(1) of section 69A of the Act and it is necessary or expedient and justifiable to block such information or part thereof and submit the request with specific recommendations in writing to Secretary, Department of Information Technology.

(2) In a case of emergency nature, the Secretary, Department of Information Technology may, if he is satisfied that it is necessary or expedient and justifiable for blocking for public access of any information or part thereof through any computer resource and after recording reasons in writing, as an interim measure issue such directions as he may consider necessary to such identified or identifiable persons or intermediary in control of such computer resource hosting such information or part thereof without giving him an opportunity of hearing.

(3) The Designated Officer, at the earliest but not later than forty-eight hours of issue of direction under sub-rule (2), shall bring the request before the committee referred to in rule 7 for its consideration and recommendation.

(4) On receipt of recommendations of committee, Secretary, Department of Information Technology, shall pass the final order as regard to approval of such request and in case the request for blocking is not approved by the Secretary, Department of Information Technology in his final order, the interim direction issued under sub-rule (2) shall be revoked and the person or intermediary in control of such information shall be accordingly directed to unblock the information for public access.

10. **Process of order of court for blocking of information.**— In case of an order from a competent court in India for blocking of any information or part thereof generated, transmitted, received, stored or hosted in a computer resource, the Designated Officer shall, immediately on receipt of certified copy of the court order, submit it to the Secretary, Department of Information Technology and initiate action as directed by the court.

11. **Expeditious disposal of request.**— The request received from the Nodal Officer shall be decided expeditiously which in no case shall be more than seven working days from the date of receipt of the request.

12. **Action for non-compliance of direction by intermediary.**— In case the intermediary fails to comply with the direction issued to him under rule 9, the Designated Officer shall, with the prior approval of the Secretary, Department of Information Technology, initiate appropriate action as may be required to comply with the provisions of sub-section (3) of section 69A of the Act.

13. **Intermediary to designate one person to receive and handle directions.**— (1) Every intermediary shall designate at least one person to receive and handle the directions for blocking of access by the public any information generated, transmitted, received, stored or hosted in any computer resource under these rules.

(2) The designated person of the Intermediary shall acknowledge receipt of the directions to the Designated Officer within two hours on receipt of the direction through acknowledgement letter or fax or e-mail signed with electronic signature.

14. **Meeting of Review Committee.—** The Review Committee shall meet at least once in two months and record its findings whether the directions issued under these rules are in accordance with the provisions of sub-section (1) of section 69A of the Act and if 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 unblocking of said information generated, transmitted, received, stored or hosted in a computer resource for public access.

15. **Maintenance of records by Designated Officer.—** The Designated Officer shall maintain complete record of the request received and action taken thereof, in electronic database and also in register of the cases of blocking for public access of the information generated, transmitted, received, stored or hosted in a computer resource.

16. **Requests and complaints to be confidential.—** Strict confidentiality shall be maintained regarding all the requests and complaints received and actions taken thereof.

FORM

[See rule 6(2)]

A. Complaint

1. Name of the complainant : --________________________________
(Person who has sent the complaint to the Ministry/Department/State Govt./Nodal Officer)

2. Address : ____________________________________
____
City : ________________ Pin Code: ____________

3. Telephone : __________ (prefix STD code) 4. Fax (if any) : __________

5. Mobile (if any): ________________________

6. Email (if any): ____________________________________

B : Details of website/ computer resource/intermediary/ offending information hosted on the website

(Please give details wherever known)

7. URL / web address : ____________________________

8. IP Address : ____________________________

9. Hyperlink : ____________________________

10. Server/Proxy Server address : ____________________________

11. Name of the Intermediary : ____________________________

12. URL of the Intermediary : ____________________________

(Please attach screenshot/printout of the offending information)

13. Address or location of intermediary in case the intermediary is telecom service provider, network service provider, internet service provider, web-hosting service provider and cyber café or other form of intermediary for which information under points (7), (8), (9), (10), (11) and (12) are not available.

____
____
____

C. Details of Request for blocking

14. Recommendation/Comments of the Ministry/State Govt : ____________

____

____

15. The level at which the comments/ recommendation have been approved (Please specify designation) : ____________

16. Have the complaint been examined in Ministry/State Government : Y/N

17. If yes, under which of the following reasons it falls (please tick):
    (i) Interest of sovereignty or integrity of India
    (ii) Defence of India
    (iii) Security of the State
    (iv) Friendly relations with foreign States
    (v) Public order
    (vi) For preventing incitement to the commission of any cognisable offence relating to above

D. Details of the Nodal Officer forwarding the complaint alongwith recommendation of the Ministry/State Govt. and related enclosures

18. Name of the Nodal Officer: ____________
19. Designation : ____________
20. organisation : ____________
21. Address : ____________

____

City : ____________ Pin Code: ____________

22. Telephone: ____________(prefix STD code) 23. Fax (if any): ____________

24. Mobile (if any): ____________

25. Email (if any): ____________

E. Any other information :

F. Enclosures :
1.
2.
3.

Date : Place: Signature

[No. 9(16)/2004-EC]
N. RAVI SHANKER, Jt. Secy.

3855GI/09-5

अधिसूचना

नई दिल्ली, 27 अक्तूबर, 2009

सा.का.नि. 782(अ).— केंद्रीय सरकार, सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 69ख की उपधारा (3) के साथ पठित, धारा 87 की उपधारा (2) के खंड (यक) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए निम्नलिखित नियम बनाती है, अर्थात, :

1. **संक्षिप्त नाम और प्रारंभ** – (1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (ट्रैफिक आंकड़ों या सूचना को मानीटर और एकत्रित करने के लिए प्रक्रिया और रक्षोपाय) नियम, 2009 है ।

(2) ये राजपत्र में प्रकाशन की तारीख को प्रवृत्त होंगे ।

2. **परिभाषाएं.** – इन नियमों में, जब तक संदर्भ से अन्यथा अपेक्षित न हो,–

(क) ''अधिनियम'' से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है ;

(ख) ''संचार'' से सूचना या संकेत का किसी रीति से प्रसारण, पारेषण, वहन अभिप्रेत है और इसके अंतर्गत प्रत्यक्ष संचार और अप्रत्यक्ष संचार दोनों हैं ;

(ग) ''संचार लिंक'' से कंप्यूटर साधन के अंतः - संयोजन करने के लिए सेटेलाइट, माइक्रोवेव, रेडियो, टेरेस्ट्रियल लाइन, तार, बेतार या किसी अन्य संचार माध्यम का उपयोग अभिप्रेत है ;

(घ) ''सक्षम प्राधिकारी'' से संचार और सूचना प्रौद्योगिकी मंत्रालय के अधीन सूचना प्रौद्योगिकी विभाग में भारत सरकार का सचिव अभिप्रेत है ;

(ङ) ''कंप्यूटर साधन'' से अधिनियम की धारा 2 की उपधारा (1) के खंड (ट) में यथा परिभाषित कंप्यूटर साधन अभिप्रेत है ;

(च) ''साइबर सुरक्षा घटना'' से साइबर सुरक्षा के संबंध में कोई ऐसी वास्तविक या संदिग्ध प्रतिकूल घटना अभिप्रेत है जो लागू सुरक्षा नीति का प्रकट रूप से या अव्यक्त रूप से अतिक्रमण करती है, जिसका परिणाम सूचना का प्रसंस्करण या भंडारण या आंकड़ों में परिवर्तन के लिए किसी कंप्यूटर साधन तक अप्राधिकृत पहुंच, सेवा से इन्कार/व्यवधान, अप्राधिकृत प्रयोग प्राधिकार के बिना सूचना में होता है ;

(छ) ''साइबर सुरक्षा भंग'' से किसी व्यक्ति द्वारा आंकड़ों या सूचना का ऐसा अप्राधिकृत अर्जन या अप्राधिकृत प्रयोग अभिप्रेत है, जो किसी कंप्यूटर साधन में अनुरक्षित सूचना की गोपनीयता, अखंडता या उपलब्धता से समझौता करता है ;

(ज) ''सूचना'' से अधिनियम की धारा 2 की उपधारा (1) के खंड (v) में यथा परिभाषित सूचना अभिप्रेत है ;

(झ) ''सूचना सुरक्षा पद्धतियों'' से साइबर सुरक्षा घटनाओं और भंगों को कम करने के लिए सुरक्षा नीतियों और मानकों को लागू करना अभिप्रेत है ;

(ञ) ''मध्यवर्ती'' से अधिनियम की धारा 2 की उपधारा (1) के खंड (ब) में यथा परिभाषित कोई मध्यवर्ती अभिप्रेत है ;

(ट) ''मानीटर'' के अंतर्गत, उसके व्याकरणिक रूपभेदों और सजातीय पदों सहित, किसी मानीटर करनेवाली युक्ति के साधनों द्वारा किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त या भंडारित ट्रैफिक आंकड़ों या सूचना को देखना या उसका निरीक्षण करना या उसे अभिलिखित करना या संग्रह करना भी है ;

(ठ) ''मानीटर करने वाली युक्ति'' से कोई इलेक्ट्रोनिक, यांत्रिक, इलेक्ट्रो - यांत्रिक, इलेक्ट्रो - चुम्बकीय, प्रकाशकीय या अन्य उपकरण, युक्ति, उपस्कर या साधित्र, जिसका या तो स्वयं या किसी अन्य उपकरण, युक्ति, उपस्कर या साधित्र के साथ संयोजन से, ट्रैफिक आंकड़ों या सूचना को देखने या निरीक्षण करने या अभिलिखित अथवा संग्रह करने के लिए उपयोग किया जाता है या उपयोग किया जा सकता है ;

(ड) ''पोर्ट'' या ''उपयोजन पोर्ट'' से ऐसे सॉफ्टवेयर नियमों का सैट अभिप्रेत है, जो उपयोजन से उपयोजन, नेटवर्क से नेटवर्क, कंप्यूटर से कंप्यूटर, कंप्यूटर प्रणाली से कंप्यूटर प्रणाली के बीच संचार का पता लगाता है और उसकी अनुज्ञा देता है ;

(ढ) ''पुनर्विलोकन समिति'' से भारतीय तार नियम, 1951 के नियम 419क के अधीन गठित पुनर्विलोकन समिति अभिप्रेत है ;

(ण) ''सुरक्षा नीति'' से सूचना और कंप्यूटर साधन का संरक्षण करने के लिए दस्तावेजीकृत कारबार, नियम और प्रक्रियाएं अभिप्रेत हैं ;

(त) ''ट्रैफिक आंकड़ों'' से अधिनियम की धारा 69ख के स्पष्टीकरण (ii) में यथा परिभाषित ट्रैफिक आंकड़े अभिप्रेत हैं ;

3. मानीटर करने के लिए निदेश.– (1) अधिनियम की धारा 69ख की उपधारा (3) के अधीन ट्रैफिक आंकड़ों या सूचना के मानीटर करने और संग्रहण के लिए कोई निदेश, सक्षम प्राधिकारी द्वारा किए गए किसी आदेश के सिवाय, जारी नहीं किया जाएगा ।

(2) सक्षम प्राधिकारी साइबर सुरक्षा से संबंधित निम्नलिखित किसी या सभी प्रयोजनों के लिए मानीटर करने के निदेश जारी कर सकेगा, अर्थात :-

(क) आसन्न साइबर घटनाओं का पूर्वानुमान करना ;

(ख) कंप्यूटर साधन पर ट्रैफिक आंकड़ों या सूचना के साथ नेटवर्क उपयोजन का मानीटर करना ;

(ग) वायरसों या कंप्यूटर संदूषकों का पता लगाना और अवधारण करना ;

(घ) साइबर सुरक्षा भंगों या साइबर सुरक्षा घटनाओं को खोज निकालना;

(ङ) साइबर सुरक्षा भंग करने वाले या वायरस फैलाने वाले कंप्यूटर साधन या कंप्यूटर संदूषकों को खोज निकालना ;

(च) किसी ऐसे व्यक्ति की पहचान करना या उसे खोज निकालना, जिसने साइबर सुरक्षा को भंग किया है या जिसके बारे में भंग करने का संदेह है या जो भंग करने की संभावना के लिए संदिग्ध है ;

(छ) कंप्यूटर साधन में सूचना सुरक्षा प्रणालियों के अन्वेषण या आंतरिक संपरीक्षा के भाग रूप में संबंधित कंप्यूटर साधन की फोरेंसिक के लिए उत्तरदायित्व ;

(ज) तत्समय प्रवृत्त साइबर सुरक्षा से संबंधित विधियों के किन्हीं उपबंधों के प्रवर्तन के लिए भंडारित सूचना तक पहुंच प्राप्त करना ;

(झ) साइबर सुरक्षा से संबंधित कोई अन्य विषय ।

(3) उपनियम (2) के अधीन सक्षम प्राधिकारी द्वारा जारी किए गए किसी निदेश में, ऐसे निदेश के लिए कारण अंतर्विष्ट होंगे और ऐसे निदेश की एक प्रति सात कार्यदिवसों की अवधि के भीतर पुनर्विलोकन समिति को अग्रेषित की जाएगी ।

(4) ट्रैफिक आंकड़ों या सूचना के मानीटर और संग्रह करने के लिए सक्षम प्राधिकारी के निदेश में किसी व्यक्ति या वर्ग के व्यक्तियों से या किसी विशिष्ट विषय से संबंधित ट्रैफिक आंकड़ों या सूचना का मानीटर और संग्रह करना सम्मिलित हो सकेगा, चाहे ऐसे ट्रैफिक आंकड़ों या सूचना या वर्ग के ट्रैफिक आंकड़ों या सूचना को एक या अधिक कंप्यूटर साधनों में प्राप्त किया जाता है, जो ऐसे कंप्यूटर साधन हैं जिनका एक विशिष्ट व्यक्ति या एक या बहुत परिसरों के सेट से या ट्रैफिक के लिए आंकड़ों या सूचना के जनन, पारेषण, प्राप्त, भंडारण करने के लिए उपयोग किए जाने की संभावना है ।

(4) ट्रैफिक आंकड़ों या सूचना के मानीटर या संग्रह करने के लिए सरकार का प्राधिकृत अभिकरण.- (1) सक्षम प्राधिकारी सरकार के किसी अभिकरण को किसी कंप्यूटर साधन में जनित, पारेषित, प्राप्त या भंडारित ट्रैफिक आंकड़ों या सूचना को मानीटर या संग्रह करने के लिए प्राधिकृत कर सकता है ।

(2) उप नियम (1) के अधीन सक्षम प्राधिकारी द्वारा प्राधिकृत अभिकरण एक या अधिक ऐसे नोडल अधिकारियों को, जो भारत सरकार के सचिव की पंक्ति से निम्न पंक्ति के न हों, नियम 3 के अधीन जारी किए गए निदेश को वहन करने वाली अध्यपेक्षा को प्राधिकृत करने और भेजनें के प्रयोजन के लिए पदाभिहित करेगा ।

(3) उप नियम (2) के अधीन अध्यपेक्षा में उस अधिकारी या अभिकरण का नाम और पदाभिधान विनिर्दिष्ट होगा, जिसको मानीटर या संग्रह किए गए ट्रैफिक आंकड़ों या सूचना को प्रकट किया जाना है ।

(4) कंप्यूटर साधन के मध्यवर्ती या भारसाधक व्यक्ति एक या अधिक अधिकारियों को ट्रैफिक आंकड़ों या सूचना का मानीटर या संग्रह करने के लिए नोडल अधिकारी से ऐसी अध्यपेक्षा प्राप्त करने और ऐसी अध्यपेक्षा के संबंध में कार्रवाई करने के लिए पदाभिहित करेंगे ।

(5) मानीटर करने के लिए निदेश पहुंचाने वाली अध्यपेक्षा को कंप्यूटर साधन के मध्यवर्ती के पदाभिहित अधिकारियों या भारसाधक व्यक्ति को नोडल अधिकारी द्वारा लिखित पत्र या फैक्स द्वारा पहुंचाया जाएगा या ऐसे अधिकारी द्वारा, जो अवर सचिव की पंक्ति से निम्न पंक्ति का न हो या समतुल्य पंक्ति का हो, परिदत्त किया जाएगा (जिसके अंतर्गत इलेक्ट्रोनिक चिह्नांकन से चिह्नित ई-मेल द्वारा परिदान भी है) ।

(6) उपनियम (2) के अधीन मानीटर करने के लिए निदेश पहुंचाने वाली अध्यपेक्षा जारी करने वाला नोडल अधिकारी मध्यवर्ती के पदाभिहित अधिकारी या कंप्यूटर साधन के भारसाधक व्यक्ति को ऐसी अध्यपेक्षा में दर्शित रूपविधान के अनुसार मानीटर करने के लिए लिखित में भी अनुरोध करेगा और उसकी रिपोर्ट उपनियम (3) के अधीन पदाभिहित अधिकारी को करेगा ।

(7) नोडल अधिकारी उपस्कर के संस्थापन, हटाने और परीक्षण करने, सभी सुविधाएं, सहयोग और सहायता देने के लिए और ऑन लाइन पहुंच को भी समर्थ बनाने या ट्रैफिक आंकड़ों या सूचना का मानीटर और संग्रह करने के लिए कंप्यूटर साधन तक ऑन लाइन पहुंच को सुरक्षित करने और उसका उपबंध करने के लिए सभी सुविधाएं, सहयोग और सहायता देने के लिए उपनियम (4) के अधीन मध्यवर्ती के अधिकारी या कंप्यूटर साधन के भारसाधक व्यक्ति से भी अनुरोध करेगा ।

(8) नियम 3 के उपनियम (2) के अधीन जारी किए गए निदेश को पहुंचाने वाली उपनियम (2) के अधीन अध्यपेक्षा की प्राप्ति पर उपनियम (4) के अधीन मध्यवर्ती का पदाभिहित अधिकारी या कंप्यूटर साधन का भारसाधक व्यक्ति, पत्र या फैक्स या इलेक्ट्रोनिक रूप से चिह्नित ई-मेल के द्वारा अध्यपेक्षा की प्राप्ति की, नोडल अधिकारी को, ऐसी अध्यपेक्षा की प्राप्ति के समय से दो घंटे की अवधि के भीतर अभिस्वीकृति देगा ।

(9) उपनियम (4) के अधीन पदाभिहित मध्यवर्ती का अधिकारी या कंप्यूटर साधन का भारसाधक व्यक्ति उसके द्वारा प्राप्त की गई अध्यपेक्षाओं का उचित अभिलेख रखेगा ।

(10) मध्यवर्ती का पदाभिहित अधिकारी या कंप्यूटर साधन का भारसाधक व्यक्ति ट्रैफिक आंकड़ों या सूचना को मानीटर या संग्रह करने के लिए निदेश पहुंचाने वाली अध्यपेक्षा की एक सूची प्रत्येक पंद्रह दिन में नोडल अधिकारी को अग्रेषित करेगा, जिसमें संबंधित सक्षम प्राधिकारी के निदेश को पहुंचाने वाली अध्यपेक्षा के निर्देश और तारीख जैसे ब्यौरे सम्मिलित होंगे ।

5. मध्यवर्ती द्वारा ट्रैफिक आंकड़ों या सूचना के मानीटर या संग्रह करने के कार्य में प्रभावी नियंत्रण सुनिश्चित करना.– मध्यवर्ती या कंप्यूटर साधन का भारसाधक व्यक्ति उस स्थान पर यह सुनिश्चित करने के लिए पर्याप्त और प्रभावी आंतरिक नियंत्रण रखेगा कि ट्रैफिक आंकड़ों या सूचना को अप्राधिकृत रूप से मानीटर या संग्रह नहीं किया जाता है और अत्यधिक गोपनीयता रखी जाती है तथा ट्रैफिक आंकड़ों या सूचना के मानीटर या संग्रह करने के मामले में अत्यधिक सावधानी और पूर्वावधानी रखी जाती है क्योंकि उससे नागरिकों के निजीपन पर प्रभाव पड़ता है और यह भी कि इस मामले में मध्यवर्ती के पदाभिहित अधिकारी या कंप्यूटर साधन के भारसाधक व्यक्ति द्वारा ही कार्रवाई की जाती है ।

6. मध्यवर्ती का उत्तरदायित्व.– मध्यवर्ती या कंप्यूटर साधन का भारसाधक व्यक्ति अपने कर्मचारियों के कार्यों के लिए भी उत्तरदायी होंगे और सूचना की गोपनीयता और विश्वसनीयता के बनाए रखने या ट्रैफिक आंकड़ों या सूचना के अप्राधिकृत रूप से मानीटर या संग्रह करने से संबंधित अधिनियम और उसके अधीन बनाए गए नियमों के उपबंधों के अतिक्रमण के मामले में मध्यवर्ती या कंप्यूटर साधन का भारसाधक व्यक्ति तत्समय प्रवृत्त विधियों के सुसंगत उपबंध के अधीन किसी कार्रवाई के लिए दायी होगा ।

7. सक्षम प्राधिकारी के निदेशों को पुनर्विलोकन.– पुनर्विलोकन समिति की बैठक दो मास में कम से कम एक बार होगी और समिति अपने उन निष्कर्षों को अभिलिखित करेगी कि क्या नियम 3 के उपनियम (2) के अधीन जारी किए गए निदेश अधिनियम की धारा 69ख की उपधारा (3) के उपबंधों के अनुसार हैं और जहां पुनर्विलोकन समिति की यह राय है कि निदेश ऊपर निर्दिष्ट उपबंधों के अनुसार नहीं है, वहां वह निदेशों को अपास्त कर सकेगा और प्रतियों के, जिनके अंतर्गत मानीटर या संग्रह किए गए ट्रैफिक आंकड़ों या सूचना का तत्संबंधी इलेक्ट्रोनिक अभिलेख भी हैं, नष्ट करने के लिए आदेश जारी कर सकेगी ।

8. अभिलेखों को नष्ट करना.– (1) प्रत्येक अभिलेख, जिसके अंतर्गत ट्रैफिक आंकड़ों का मानीटर या संग्रह करने के लिए ऐसे निदेशों से संबंधित इलेक्ट्रोनिक अभिलेख भी हैं, निदेश की प्राप्ति या अभिलेख के सृजन से, जो भी पश्चात्वर्ती हो, नौ मास की अवधि की समाप्ति के पश्चात, सिवाए उस दशा के जहां ट्रैफिक आंकड़े या सूचना कृत्यकारी अपेक्षाओं के लिए अपेक्षित है या होने की संभावना है, नष्ट कर दिया जाएगा ।

(2) किसी चल रहे अन्वेषण, आपराधिक परिवाद या विधिक कार्यवाहियों के प्रयोजन के लिए अपेक्षित से अन्यथा के सिवाय मध्यवर्ती कंप्यूटर साधन का भारसाधक व्यक्ति सूचना के मानीटर करने या संग्रह के निदेशों से संबंधित अभिलेखों को, ट्रैफिक आंकड़ों का मानीटर करना या संग्रह बंद किए जाने के छह मास की अवधि के भीतर नष्ट करेगा ।

9. प्राधिकार के बिना ट्रैफिक आंकड़ों या सूचना को मानीटर या संग्रह करने का प्रतिषेध.– (1) कोई व्यक्ति, जो साशय या जानबूझकर, नियम 3 के उपनियम (2) या नियम 4 के उपनियम (1) के अधीन प्राधिकार के बिना ट्रैफिक आंकड़ों या सूचना का भारत के भीतर किसी स्थान पर उसके होने या पारेषण के अनुक्रम में मानीटर या संग्रह करता है या ट्रैफिक आंकड़ों या सूचना का मानीटर करने या संग्रह करने का प्रयास करता है या ट्रैफिक आंकड़ों या सूचना का मानीटर या संग्रह करने के लिए किसी व्यक्ति को प्राधिकृत करता है या उसकी सहायता करता है, उसके विरुद्ध कार्यवाही की जाएगी उसे तत्समय प्रवृत्त विधि के सुसंगत उपबंधों के अधीन तदनुसार दंडित किया जाएगा ।

(2) कंप्यूटर साधन में ट्रैफिक आंकड़ों या सूचना का किसी मध्यवर्ती के कर्मचारी या कंप्यूटर साधन के भारसाधक व्यक्ति द्वारा या मध्यवर्ती द्वारा सम्यक रूप से प्राधिकृत व्यक्ति द्वारा मानीटर या संग्रह उस मध्यवर्ती द्वारा प्रदाय की गई सेवाओं से संबंधित उसके कर्तव्य के अनुक्रम में किया जा सकेगा, यदि ऐसे कार्यकलाप प्रवृत्त उद्योग पद्धतियों के अनुसार उसके कर्तव्यों के निर्वहन के लिए निम्नलिखित मामलों के संबंध में युक्तियुक्त रूप से आवश्यक हैं :-

(i) कंप्यूटर साधन का या कंप्यूटर साधन के साथ प्रयोग किए जाने वाले किसी उपस्कर का संस्थापन ;

(ii) कंप्यूटर साधन का प्रचालन या अनुरक्षण ; या

(iii) मध्यवर्ती या अभिदाता के सिरे पर किसी संचार लिंक या सॉफ्टवेयर का संस्थापन या मध्यवर्ती के कंप्यूटर साधन पर उपयोगकर्ता लेखा का संस्थापन और उसकी कृत्यकारिता के लिए उसका परीक्षण ;

(iv) उपस्कर, कंप्यूटर साधन या किसी संचार लिंक या कोड के संस्थापन, संयोजन या अनुरक्षण से संबंधित कंप्यूटर साधन से भंडारित सूचना तक पहुंच प्राप्त करना ; या

(v) कंप्यूटर साधन से निम्नलिखित प्रयोजन के लिए भंडारित सूचना तक पहुंच प्राप्त करना :

(क) कंप्यूटर साधन में सूचना सुरक्षा पद्धतियों का कार्यान्वयन ;

(ख) सुरक्षा भंगों, कंप्यूटर संदूषकों या कंप्यूटर वायरस का अवधारण करना ;

(ग) अन्वेषण या आंतरिक संपरीक्षा के भाग रूप में संबंधित कंप्यूटर साधन की फॉरेंसिक का उत्तरदायित्व लेना ; या

(vi) कंप्यूटर साधन या किसी व्यक्ति को, जिसने अधिनियम के किसी उपबंध का उल्लंघन किया है या जिसके बारे में उल्लंघन करने का संदेह है या जो उल्लंघन करने के लिए संभाव्य है, जिससे मध्यवर्ती द्वारा प्रदाय की गई सेवाओं पर प्रतिकूल प्रभाव पड़ने की संभावना है, खोजने के प्रयोजन के लिए कंप्यूटर साधन से सूचना तक पहुंचना या उसका विश्लेषण करना ।

(3) मध्यवर्ती या कंप्यूटर साधन का भारसाधक व्यक्ति और उसके कर्मचारी उपनियम (2) के अधीन यथाविनिर्दिष्ट कार्यों का पालन करते हुए कड़ी गोपनीयता और विश्वसनीयता रखेगा ।

(4) मानीटर किए गए या संग्रहित ट्रैफिक आंकड़ों या सूचना के ब्यौरों का मध्यवर्ती या कंप्यूटर साधन के भारसाधक व्यक्ति या उसके किसी कर्मचारी द्वारा उपयोग नहीं किया जाएगा या उसे नियम 4 के उपनियम (2) के अधीन उक्त सूचना के आशयित प्राप्तकर्ता से भिन्न किसी व्यक्ति को प्रकट नहीं किया जाएगा । किसी मध्यवर्ती या उसके कर्मचारी या कंप्यूटर साधन के भारसाधक व्यक्ति के विरुद्ध, जो इस नियम के उपबंधों का उल्लंघन करता है, कार्रवाई की जाएगी और उसे इस अधिनियम या तत्समय प्रवृत्त किसी अन्य विधि के सुसंगत उपबंधों के अधीन तदनुसार दंडित किया जाएगा ।

10. प्राधिकृत अभिकरण द्वारा ट्रैफिक आंकड़ों के या सूचना के प्रकट करने का प्रतिषेध.— मानीटर किए गए या संग्रहित ट्रैफिक आंकड़ों या सूचना के ब्यौरों का नियम 4 के उपनियम (1) के अधीन प्राधिकृत अभिकरण द्वारा किसी अन्य प्रयोजन के लिए, आसन्न साइबर खतरों या इंटरनेट पर पोर्ट - अनुसार ट्रैफिक के साधारण रुझानों का पूर्वानुमान लगाने या साइबर घटनाओं के साधारण विश्लेषण या अन्वेषण के लिए अथवा भारत में सक्षम न्यायालय के समक्ष न्यायिक कार्यवाहियों में के सिवाय, उपयोग नहीं किया जाएगा या उसे प्रकट नहीं किया जाएगा ।

11. विश्वसनीयता का बनाए रखा जाना—नियम 10 में यथा अन्यथा उपबंधित के सिवाए इन नियमों के अधीन सक्षम प्राधिकारी द्वारा जारी किए गए ट्रैफिक आंकड़ों या सूचना को मानीटर करने या संग्रह करने के लिए निदेशों के संबंध में कड़ी गोपनीयता रखी जाएगी ।

[सं. 9(16)/2004 ई.सी.]

एन. रवि शंकर, संयुक्त सचिव

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.

[No. 9(16)/2004-EC]
N. RAVI SHANKER, Jt. Secy.

Printed by the Manager, Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.