REGULATION
on the functionality of public communications networks

CHAPTER I
Objective and scope

Article 1
Objectives

The objective of this Regulation is to increase consumer protection and strengthen the foundations of the information society. This Regulation stipulates the measures that the Post and Telecom Administration considers it necessary that electronic communications undertakings adopt in order to guarantee continuous operation of public communications networks. According to the Regulation, measures must be adopted with respect to carrying capacity, alternate paths, management, and external environment of networks. Furthermore, there must be measures concerning emergency plans for the purpose of responding to unforeseen circumstances, mitigating their effects, and facilitating the rapid, efficient restoration of equipment or service.

Article 2
Scope

This Regulation applies to the functionality of public communications networks – that is, the actual electronic communications networks, together with the information systems on which they depend and to which they are connected – as these lie within the scope of the Electronic Communications Act, no. 81/2003. The Regulation applies to electronic communications undertakings offering publicly accessible electronic communication services.

It applies to all public communications networks, up to and including the network termination points within the intake; however, it does not apply to cables, equipment, and infrastructure on the premises of the customer. Internal cabling is discussed separately in the Post and Telecom Administration Regulation on Indoor Cables for Electronic Communications, no. 1109/2006.

Article 3
Definitions

The words and terms in these regulations shall mean the following:

Access control: A method for ensuring that only authorised parties have access to an electronic communications network; for example, to defined areas or data, whether these are in electronic form or not.

Alternate traffic path: A path, in addition to the main traffic path, that is always functional and transfers a portion of the traffic or is activated if needed.

Availability: Means that data are accessible and services are operational, or as possible in cases of power outage, natural disaster, accident, or network attack.

Computer Security Incidents Response Team (CSIRT): A team that works toward safeguarding against security incidents, unstable functionality, and suspicious incidents in information systems and electronic communications networks in Iceland.

Confidentiality: The protection of communications or stored data against interception and reading by unauthorised persons.

Critical infrastructure that affects national security: Electronic communications infrastructure concerning which security incidents, precarious functionality, or suspicious events could affect national security; that is, could affect other national infrastructure, jeopardise public safety, threaten economic or social equilibrium, or cause instability in the government or defence of the nation.

Critical infrastructure: The electronic communications network infrastructure that forms the foundation for the electronic communications network as a whole and for the electronic communications services rendered; for example, the innermost core of the electronic communications network and the main network traffic paths, including paths to interconnections abroad. Unstable functionality of such infrastructure could threaten the public's trust in the service rendered by the electronic communications undertaking concerned, and in electronic communications as a whole.

Electronic communications network: Transmission systems and, where applicable, switching or routing equipment and other resources that permit the conveyance of signals by wire, radio, by optical or by other electromagnetic means, including networks for radio and television broadcasting and cable television networks.

Electronic communications service: Means a service that consists wholly or mainly of the conveyance of signals on electronic communications networks, including e-mail services and network access.

Electronic communications undertaking: An individual or legal entity that has notified the Post and Telecom Administration of proposed operation of electronic communications services or electronic communications networks.

Information: Any sort of symbol, signal, writing, image, and sound that is sent or received, and any sort of communication through cables, by radio or other electromagnetic systems.

Integrity: The confirmation that data that have been sent, received, or stored are complete and unchanged.

IP electronic communications network: An electronic communications network that transfers data packets in accordance with IP (Internet Protocol) standards.

IP electronic communications services: Electronic communications services that are provided on a public IP electronic communications network, such as e-mail service, web services, name service, file transfer, chat rooms, etc. Also included are operational elements such as domain hosting and IP network registration.

Main traffic path: A high-capacity path in an electronic communications network that transfers significant traffic between individual parts of the network; for example, traffic for a large group of customers.

Malicious code: Software or programming modules that become lodged in computers and electronic communications networks for the purpose of performing unauthorised or damaging operations. Examples of malicious code are computer viruses and worms.

Malicious traffic: Electronic communications traffic that is sent for the purpose of harming network functionality. Examples of malicious traffic are denial of service attacks and excessive unsolicited bulk e-mail.

Network access: The actual availability of electronic communications networks and related services, including services that authenticate users, identification services, and proxy transfer. It also refers to support services rendered, such as the provision of IP addresses, domains, and web services.

Network and information security: The ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.

Network attack: An attack launched on an electronic communications network, aimed at curtailing services or interfering with the functionality of networks and systems.

Network switch: Equipment that, among other things, divides networks into virtual networks.

Network termination point: The physical connection point where the subscriber is granted access to a public communications network.

Physical: Refers to a tangible item or a real environment.

Proxy transfer: An intermediary in the transfer of customers' electronic communications traffic, which generally hides the registered IP address of the sender and shows instead the intermediary's IP address; for example, so-called proxy service.

Public communications network: An electronic communications network that is used wholly or mainly for the provision of electronic communications services available to the public.

Router: Equipment whose primary function is to direct data packets along the proper routes.

Security event: An identified occurrence of a system, service or network state indicating a possible breach of security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

Security incident: A security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Switching system: A system on an electronic communications network that handles the administration and transfer of circuit-switched traffic, including that for voice calls.

CHAPTER II
General requirements and instructions

Article 4
General

This Regulation sets forth the requirements made of electronic communications undertakings with respect to guaranteeing the functionality and security of public communications networks; that is, the actual electronic communications networks and the information systems to which they are connected and on which they depend, such as accounting and access control applications, hereinafter referred to as electronic communications networks. With respect to the requirements that are not stated explicitly in this Regulation, electronic communications undertakings shall identify them through a structured risk assessment and shall have in place measures to control and

administer electronic communications networks with regard to risk. It is permissible to use the standards ISO/IEC 27001 (Information security management systems) and ISO/IEC 17799 (Code of practice for information security management) for reference. The most recent version of the standards must be used at any given time. The standards may also be used as a guideline for measures to be implemented in order to meet the requirements set forth in the Regulation.

Article 5

Adherence to standards

More detailed technological information on the implementation of provisions in this Regulation is set forth in the ITU standards, which have been translated and issued by IST – Icelandic Standards. If translations are not available, the English version of the ITU standards shall be used if they are available. In other respects, the guidelines for the ITU, ISO, or IEC standards or other recognised and available documents shall be used as a reference; for example, those issued by IEFT. The same applies to topics outside the scope of these Rules.

CHAPTER III

Business continuity plans and testing

Article 6

General

Electronic communications undertakings shall prepare a business continuity plan based on risk assessment. They shall carry out internal controls that include an assessment of the effectiveness of the business continuity plans.

Article 7

Impact analysis and risk assessment

Electronic communications undertakings shall use impact analysis and risk assessment in order to reduce all major weaknesses and vulnerabilities in their infrastructure.

The impact analysis focuses on incidents that could cause interruption of service due to, among other things, malfunction, mishap, or other threats to an undertaking's security; for example, natural disaster, internecine epidemic, accident, power outage, equipment failure, burglary, vandalism, etc.

The risk assessment shall evaluate the probability of such incidents and shall estimate their impact, considering the weaknesses inherent in electronic communications operations and electronic communications networks.

In particular, the risk assessment shall analyse all critical infrastructure. It shall describe the use of all critical infrastructures and the interconnection of such infrastructures with other parts of the electronic communications network, as well as with other electronic communications networks. It shall also describe how the security of critical infrastructure is best safeguarded, including protection against power outages, describe information and monitoring systems, alternative traffic paths, stand-by equipment, service agreements, actions against security incidents, physical protection, and backup and resumption procedures.

In other respects, the risk assessment shall be carried out in accordance with the guidelines set forth in Article 7 of the Post and Telecom Administration Regulation on the Protection of Information in Public Communications Networks, no. 1221/2007.

Article 8

Business continuity plan

Plans must be in place so as to guarantee continuous, uninterrupted operation of electronic communications networks and services. To that end, electronic communications undertakings shall prepare a written business continuity strategy based on the results of the business continuity risk assessments. According to the strategy, business continuity plans shall include a description of measures to recover inoperative electronic communications networks and restoration of any data that may have been damaged or lost. The business continuity plans shall be tested on a regular basis so as to guarantee their effectiveness. The plans shall include the following, at a minimum:

1. A description of the structure and sphere of responsibility of individual emergency teams.
2. A description of the maintenance of manuals for the daily operation of equipment.
3. Operational procedures to follow to carry out emergency solutions.
4. A definition of the maximum down time before the continuity plans will be implemented.
5. Information on the principal contact personnel for suppliers and service providers.

Article 9

Internal control

Monitoring shall be carried out so as to guarantee the effectiveness of the business continuity plans. It shall be carried out systematically in accordance with a pre-defined maintenance schedule. Procedures that guarantee uninterrupted operations shall be maintained and shall always reflect actual operational requirements insofar as is possible. The frequency and scope of the monitoring shall be determined with reference to defined risk and the significance of the electronic communications networks in question, the technology used to guarantee their security, and the cost incurred in carrying out the monitoring procedures. The monitoring procedures shall be carried out at least once a year, however. Monitoring and updating of the business continuity plan's effectiveness shall be a part of regular internal controls.

CHAPTER IV
Physical protection

Article 10

Electronic communications network perimeters

The physical security of electronic communications networks perimeters shall reflect the importance of the electronic communications networks and other electronic communications equipment housed in areas within that perimeter, according to a risk assessment. Access control and other necessary measures shall be adopted; for example, protection against moisture, water leakage, heat, or fire. Adequate work facilities and operational procedures shall be in existence.

At a minimum, the following measures shall be adopted, as appropriate, for perimeters used to house critical infrastructure as described in the risk assessment:

1. Unauthorised access to the perimeter shall be prevented with secure doors and locks.
2. Employees and contractors shall be identified.
3. Access by employees and contractors shall be controlled with access cards or comparable identification procedure.
4. Guest access shall be controlled so as to prevent unauthorised access.

5. The perimeters shall be constructed of non-flammable material.
6. The access control system for the perimeter shall report events and trace them to specific access control units.
7. Attempts shall be made to have no windows on the exterior walls of the space; otherwise, measures must be taken to prevent burglary.
8. The perimeters shall be equipped with humidity sensors that are independent of external energy sources.
9. The perimeters shall be furnished with equipment that reports fire to a central control center and issues a warning if environmental conditions change so that they no longer conform to the conditions for which the equipment is designed.
10. The perimeters shall be equipped with surveillance and an intrusion detection system that sends information to the surveillance or control center of the monitoring entity.

Article 11

Electronic communications equipment

The electronic communications network computers and equipment that are defined as critical in the risk analysis – such as traffic control and management equipment, power supplies, network switches, routers, switching systems, and cables – shall be protected with cabinets, cable trays, or cable runs. In other respects, the manufacturer's instructions shall be followed; for example, as regards the proper temperature and humidity level for the equipment.

Article 12

Electronic communications cabling

Cables between locations shall be protected with the following measures, as appropriate:

1. Exterior interconnections and cable ends, as well as connections that pass through areas controlled by a third party, shall be protected against unauthorised access.
2. Exterior access connections, together with necessary equipment, shall be protected against unauthorised access; for example, in locked street cabinets or junction boxes.
3. Exterior access to trunk lines through manholes shall be limited, and their importance shall be camouflaged.

CHAPTER V
Functionality requirements

Article 13

Capacity and operational security of traffic paths

In order to enhance operational security on main traffic paths, electronic communications undertakings shall, insofar as is possible, use backup traffic paths for the electronic communications services they provide, and there shall be physical separation between the two as much as possible.

If traffic is limited for any reason, due to insufficient transfer capacity on the backup or main traffic paths, the traffic that best serves the public interest shall be guaranteed highest priority; such as traffic for mobile phone, internet phone, and other voice call services.

For the same purpose, it is required that there will be an active backup traffic path with a separate intake between locations, and perimeters, together with the appropriate equipment, on the following electronic communications networks:

1. On fixed-line phone networks; for example, traffic paths to interconnections abroad, on high-capacity main traffic paths within local areas, or at interconnections with other electronic communications undertakings' exchange systems.
2. In mobile phone networks, on main traffic paths between mobile telephone exchanges, or to other exchange systems.
3. On main traffic paths that transfer public internet phone services provided by the electronic communications undertaking concerned.
4. On main traffic paths used for public IP electronic communications networks or other data connections, including interconnection between electronic communications undertakings. This does not apply to smaller internet service providers.

Electronic communications undertakings that operate their own international traffic paths shall specify clearly, both on their websites and in their customer agreements, what measures they take concerning backup traffic paths and how long it takes to activate them in the event of a failure on the main traffic path.

Article 14

Performance and capacity of equipment

Electronic communications network equipment shall have sufficient performance and capacity, so that it meets the requirements for the proposed usage. Measures shall be taken to prevent attacks and break-ins by hackers who could disturb electronic communications network operations.

Electronic communications undertakings shall guarantee that they have sufficient personnel and operational measures to maintain and protect the performance of critical transmission and switching systems, individual components of such systems, distribution frames, base stations, antennas and other comparable equipment. The maintenance and protection of this capacity must be set forth in advance in a capacity plan, and personnel must receive the appropriate training.

Article 15

Performance of fixed-line phone networks

The performance of the fixed-line phone network must be determined so that the proportion of customer calls that cannot be completed will never exceed 2.5% of all calls placed in a year. Televotings or other comparable activities that generate heavy traffic to specific phone numbers on a temporary basis shall not disturb other functionality – for example, other telephone traffic – unless customers are notified of possible disturbances, in accordance with Article 24 of the Regulation.

Article 16

Performance of other public communications networks

Requirements concerning the performance of other electronic communications networks shall be determined in accordance with the applicable standards.

CHAPTER VI
Management of electronic communications networks

Article 17
Management of service quality

Even though an electronic communications undertaking outsources one or more parts of its electronic communications network operations, it remains responsible for the functionality, quality, and capacity of those networks.

Article 18
Decision on equipment and structure of electronic communications networks

In electronic communications networks, the operator shall, in general, use widely accepted equipment and maintain effective, organised network arrangements that facilitate functionality and efficient network control. The parts of the electronic communications network that are defined as critical infrastructure in the risk assessment shall have absolute priority with respect to operational security, and the network structure shall be arranged accordingly.

A backup power supply shall be in place so as to support continuous electronic communications network functionality in the event of a power outage. In respect to, other than those provided for in this Regulation, the backup power supply and network arrangements shall provide for up time in accordance with the results of the risk assessment. Special emphasis shall be placed on protecting critical infrastructure with sufficient backup power. Furthermore, there shall be a sufficient number of portable power generators.

Article 19
Traffic control

For the purpose of enhancing reliability, insofar as the arrangement and capacity of the electronic communications networks allow, electronic communications undertakings shall use trustworthy equipment for network and traffic control. This equipment must be able to abandon temporary operations, such as the activation of backup traffic paths, and restore the electronic communications network to normal working condition.

Article 20
Maintenance of electronic communications networks

While electronic communications networks are in use, electronic communications undertakings shall maintain their operation and services and shall restore them quickly to full functionality after a failure.

It must be guaranteed that backup copies of the most recent equipment configuration that is necessary to restore the electronic communications network and related systems are available. Backup data shall be stored in a secure location.

As soon as it is known that specific equipment is causing a disturbance to electronic communications operations, measures shall be taken in order to restore that equipment to its previous condition or disconnect it from the network if necessary.

Insofar as is appropriate, electronic communications undertakings shall have backup equipment and other measures sufficient to maintain uninterrupted operations.

Article 21

Preventative maintenance

In order to reduce the likelihood of equipment malfunction, electronic communications undertakings shall carry out preventative maintenance of their equipment in accordance with a pre-determined schedule.

Article 22

Management of disturbances and failures

Based on failure and disturbance reports, or alert messages from equipment, electronic communications undertakings shall be able, at any time of day or night, to take the measures necessary to repair failures that cause substantial disturbance of traffic and service.

In order to restore electronic communications network operations in the shortest time possible, clear instructions shall be included in the business continuity plan. It shall also state clearly the responsibility of each individual, and include necessary contact information for repair technicians, information on spare equipment, procedures for notifications, and instructions for temporary measures to protect emergency traffic. To this end, the service and operations desk shall have instructions concerning co-operation with other service and operations desks.

Clocks in electronic communications network equipment, shall be synchronised to facilitate synergy and traceability of operations.

Reports on failures and disturbances shall be maintained so as to assist in repair and in preventative maintenance, and to investigate the service quality and performance capacity of the electronic communications networks.

In electronic communications networks management, procedures shall exist in order to notify other electronic communications undertakings of important technological issues and disturbances that will affect interconnected traffic between their networks.

Article 23

Change management in electronic communications networks

Procedures for modifications shall apply to all changes that could affect the electronic communications networks and shall guarantee the appropriate formal handling and documentation of the modifications made. The procedures shall facilitate reliable, organised, and predictable operation of the electronic communications networks concerned.

Changes shall be carried out so that they cause minimal disturbance, both to the electronic communications services of the undertaking in question and to other electronic communications undertakings.

If the changes have an unavoidable effect on the networks and services of other undertakings, the parties shall co-operate in the arrangement of the changes so as to minimise the disturbance.

Article 24

Notifications of interrupted functionality

Electronic communications undertakings shall have in place clear and effective procedures for reporting interrupted functionality or the risk of interruption in their electronic communications networks as a result of disturbances, failures, changes, and the like. Customers shall be notified of such instances, and the relevant service criteria shall appear on the undertaking’s website or in a comparable medium; for example, in customer agreements. The notification shall state, at a minimum, what effect the incident has, or may have, the measures that the electronic communications undertaking will take, and advice to customers if such an incident occurs.

Data concerning interrupted operations and other security incidents involving critical infrastructure that affect national security in electronic communications networks, shall be forwarded to entities that have a particular role to carry out in such instances. The Post and Telecom Administration shall define further what infrastructure this involves, what entities must be notified, and what data is involved.

CHAPTER VII
Security incidents

Article 25
Malicious code

If an electronic communications undertaking considers that malicious traffic or malicious code on its electronic communications network jeopardises the operation of the critical infrastructure of the network, it is authorised to take the necessary precautionary measures, such as filtering out such traffic or closing connections. The terms and conditions of the customer agreement shall state that the undertaking is authorised to take such measures. The electronic communications undertaking in question shall then send the Post and Telecom Administration a report on such incidents within 24 hours of their occurrence. The report shall describe the sequence of events, the amount and scope of data deleted, and an assessment of the impact of the incident if these measures had not been taken.

Article 26
Notification of security incidents

Customers must be notified of serious security incidents in electronic communications networks. The service criteria for such notifications shall be in accordance with Article 24, Paragraph 1.

In order to enhance the integrity and security of electronic communications networks, the Post and Telecom Administration may decide that specified data concerning security incidents that could jeopardise electronic communications network operations must be submitted to a computer security incident response team or a coordination center that operates in accordance with Article 25 of the Regulation on Protection, Functionality, and Quality of IP Electronic Communications Services, no. 1223/2007.

CHAPTER VIII
Miscellaneous provisions

Article 27
Access to information

The Post and Telecom Administration sends out questionnaires that must be answered by a specified deadline, provided that the majority of the answers can be found in the undertakings' documents. These questionnaires centre on technological and administrative matters, among other things. They also focus on items related to malfunctions, including plans and reports on interrupted operations or disturbances in service. After the questionnaires have been returned, the Post and Telecom Administration monitoring agents announce a visit to the electronic communications undertaking if they consider it necessary. The electronic communications undertaking shall provide the Post and Telecom Administration or its representative with other information, such as information on security systems. This may include the information security policy, the results of the risk assessment, a description of security measures, and internal control reports. Electronic communications undertakings must furnish this information whenever the Post and Telecom Administration requests it. Furthermore, the Administration may request further explanations and

data concerning specific security incidents or disturbances that can occur in electronic communications undertakings operations.

Article 28

Public disclosure

Electronic communications undertakings shall disclose publicly – for example, on their website – their policy on the functionality and security of their electronic communications networks. The following information must appear, at a minimum:

1. The undertaking's security policy.
2. The undertaking's policies on average up time, average restore time, and maximum utilisation of its various electronic communications networks.
3. Instructions for consumers, informing them of how they can submit comments to the undertaking if they consider the security and functionality of its electronic communications networks lacking.

Article 29

Testing and audits

The Post and Telecom Administration is authorised to test the functionality of electronic communications networks and conduct audits of whether electronic communications undertakings are in compliance with this Regulation. It may carry out such testing and audits on its own initiative or in response to a submitted comment. Testing applies to electronic communications networks, electronic communications services, and related information systems, among other things. The Administration shall decide how the testing or audits are to be carried out.

The Post and Telecom Administration may decide to engage an independent professional to carry out the audits and submit a report containing the results to the Administration. The auditor shall be obliged to observe confidentiality concerning his work for the Administration. Electronic communications undertakings shall have the option of commenting on the Administration's choice of auditor.

Article 30

Entry into force

This Regulation shall take effect on 1. July 2008.

Article 31

Authority

The Post and Telecom Administration has issued this Regulation on the Functionality of Public Communications Networks pursuant to the authority contained in Article 9(b) of Act no. 39/2007 amending the Electronic Communications Act, no. 81/2003.

Post and Telecom Administration, Iceland, 10 December 2007.

Hrafnkell V. Gíslason
Björn Geirsson.

Section B – Date of issuance: 21 December 2007