REGULATION

on the protection of information
in public communications networks

CHAPTER I
Objective and scope

Article 1
Objectives

The objective of this Regulation is to enhance consumer protection and strengthen the foundations of the information society by making increased requirements concerning the security of the electronic communications systems used by businesses and individuals. This Regulation stipulates the measures that the Post and Telecom Administration considers it necessary that electronic communications undertakings adopt in order to guarantee the protection of traffic and information in public communications networks. According to this Regulation, attempts must be made to guarantee the confidentiality, availability and integrity of information, and of lawful access to it. Enhanced security is achieved through measures that control access to information and through increased protection of electronic communications networks and services.

Article 2
Scope

This Regulation applies to network and information security in electronic communications networks – that is, the actual electronic communications networks, together with supporting and connected information systems – within the scope of the Electronic Communications Act, no. 81/2003. The Regulation applies to electronic communications undertakings that operate electronic communications services on public communications networks.

It applies to all public communications networks, up to and including the network termination points within the intake; however, it does not apply to internal 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.

The standards ISO/IEC 27001 (Information security management systems) and ISO/IEC 17799 (Code of practice for information security management) can be used 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.

With respect to the security of personal information, the provisions of Articles 11-13 of the Act on the Protection of Privacy as Regards the Processing of Personal Data, no. 77/2000, and the Regulation on the Security of Personal Data, no. 299/2001, shall apply.

Article 3
Definitions

The words and terms used in this Regulation 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.

Availability: Means that data are accessible and services are operational when they are needed, 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.

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: A service which consists wholly or mainly in 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 (PTA) of the proposed operation of electronic communications services or an electronic communications network.

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 services: Websites, file transfer, chat rooms, and other data that are transferred over an IP electronic communications network.

Messages: Telephone calls, e-mails, text messages, voice messages, image messages, television programming, IP services, or other comparable message information transferred between parties or to unidentified recipients on an electronic communications network.

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 transferred 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 causing denial of services or interference with the functionality of networks and systems.

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

Non-repudiation: A method that ensures that the sender of information cannot deny having sent specific information or that the recipient cannot deny having received it.

Physical: Refers to a tangible, material 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.

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.

CHAPTER II
General requirements and instructions

Article 4
General

Electronic communications undertakings shall adopt the appropriate measures to guarantee the protection of the public communications services and electronic communications networks that they operate, including information transmitted on such networks, against unlawful destruction, loss, or modification, either by accident or due to unauthorised access. These measures shall guarantee a suitable level of security, considering the involved risk, the level of technology, and the cost of the measures concerned.

Article 5
Confidentiality in electronic communications

Electronic communications undertakings shall ensure that their customers are protected against eavesdropping, wiretapping, storage, or other kinds of interference or surveillance of electronic communications – including messages and authentications – that take place on their electronic communications networks, unless these take place with the consent of the customer involved or in accordance with statutory authority. Any temporary technical storage which is necessary for the transmission of a communication during transfer shall be exempt from this provision, provided that the contents are not publicised in any way.

Furthermore, it must be guaranteed that an electronic communications undertaking's storage of or access to data in the customer's terminating equipment is authorised only if the user is given clear and cogent information on the purpose of such storage or access and has the opportunity to refuse it. This shall be authorised, however, for the sole purpose of carrying out the communication transmission over an electronic communications network, or as a part of regular updates.

Article 6

Integrity of information

Electronic communications undertakings shall guarantee the integrity of their customers' information so that the information is not subject to modification. This applies both to information being transferred on a public communications network and to other electronic communications information.

Article 7

Organization of security

Electronic communications undertakings shall prepare and maintain a documented description of the management system that guarantees information security in their electronic communications services and networks. This information security management system shall involve the following, at a minimum:

1. Electronic communications undertakings shall set a written *security policy*. The policy shall include a general description of the attitude of the undertaking's management toward security matters. The policy shall also state the objectives and principles of information security in accordance with the undertaking's operational policy and objectives. The policy shall be communicated to all employees of the electronic communications undertaking who are involved in electronic communications operations. In formulating the security policy, consideration shall be given to what information shall be protected, how it should be protected, the method that will be used to process it, and who is to bear responsibility for its security. The security policy shall be presented to employees.
2. The electronic communications undertaking shall define the methodology used for a *risk assessment* pertaining to information security. This methodology shall be followed up with a written risk assessment concerning information security as it relates to electronic communications networks and services. The risk assessment shall identify risk factors, define their scope, and prioritise them based on acceptable risk levels and the objectives that are most important for the undertaking. The risk assessment shall define assets and carry out a simple assessment of the assets and the effect of a possible interruption of confidentiality, integrity, or availability. Significant vulnerabilities and threats are defined for the assets and the probability of their occurrence estimated. The risk for each item is calculated and compared to a pre-calculated scale of acceptable risk levels with respect to information security, business continuity and service levels. The objective of the risk assessment is to create premises for the selection of security measures. The risk assessment shall be reviewed on a regular basis.
3. Electronic communications undertakings shall set operating procedures concerning secure handling and deletion of information. They shall formulate *security measures* and prepare written descriptions of them. They shall specify what security measures will be applied and how they will be structured, including measures concerning the design, development, operation, testing, and

maintenance of each system. They must also specify how they will respond to emergency situations pertaining to the operation of their electronic communications networks and services. Security measures shall be reviewed regularly. Written instructions shall be available for individual processes that are necessary to the information security of the electronic communications networks and services. The electronic communications undertaking shall ensure that the provisions of the information security policy are fulfilled, even when contractors work for the company. The electronic communications undertaking shall ensure that its employees follow the information security policy.

Article 8

Internal control

Internal control shall be carried out so as to guarantee that work is done according to the information security policy and the documented procedures and rules pertaining to the security structure, and to guarantee that the security structure is consistent with regulatory requirements. Internal control shall be carried out systematically in accordance with a pre-defined method. The frequency and scope of internal control shall be determined with reference to defined risk, the nature of the electronic communications networks in question, the technology used to guarantee their security, and the cost incurred in implementing the monitoring procedures. However, the internal control procedures shall be carried out at least once a year. Electronic communications undertakings shall prepare a report containing the results of internal controlling procedures.

CHAPTER III
Security measures

Article 9

Business continuity plans

Special measures shall be taken in order to guarantee the security of information in case of an interruption in service due to, for example, failure, mishap, or other incidents that could jeopardise the security of electronic communications networks. The Post and Telecom Administration sets further stipulations concerning such measures in the Regulation on the Functionality of Public Communications Networks, no. 1222/2007.

Article 10

Measures concerning employees

In order to prevent or limit loss due to mistake, fraud or other misuse, electronic communications undertakings shall, at a minimum, adopt the following measures concerning employees who, due to the nature of their work, have access to information on electronic communications networks:

1. Investigate to determine whether there is reason to require that the applicant submit a police clearance certificate before employment is offered.
2. Require that employees sign a statement of confidentiality.
3. Inform employees of their responsibilities pursuant to Chapter IX of the Electronic Communications Act, no. 81/2003.
4. Electronic communications undertakings shall define the responsibilities and obligations of their employees with respect to information security. Division of labour and responsibility for the execution of various processes relating to security shall be clearly defined, and the examination of

information must be formally prohibited unless carried out in a work-related context.

5. Guarantee that employees are informed, in a regular and systematic manner, of their work-related duties and obligations and of the consequences of violating those duties and obligations.
6. Employees shall be provided with appropriate education and training in matters related to information security.
7. Electronic communications undertakings shall examine the risk related to key information security personnel and, among other things, shall guarantee that it is always possible to contact those persons or their substitutes in an emergency.

Article 11

Access control

In order to prevent or limit loss due to unauthorised physical access, such as access to facilities or equipment, electronic communications undertakings shall, at a minimum, adopt the following measures, as appropriate:

1. Control access to buildings and equipment for electronic communications networks through the distribution of access cards, passwords, or other satisfactory means wherever possible.
2. Physically separating electronic communications equipment – such as transmitters, switching systems, and other infrastructure – from other equipment; for example, by placing such equipment in closed cabinets. This measure does not prevent an electronic communications undertaking from practising joint utilisation of facilities, however.
3. Service providers with third-party status shall only be granted limited access to critical areas when such access is necessary. Such access shall be subject to authorisation and, if necessary, monitoring.

Article 12

Organizational and technological measures

Electronic communications undertakings shall adopt the necessary technological and organizational measures to protect their public communications networks. Electronic communications undertakings shall, among other things, adopt the following measures, as appropriate:

1. Network controls for electronic communications equipment shall be protected against unauthorised access to control data and equipment identification during transport; for example, with the use of cryptographic controls or in closed management networks.
2. Use access authorisations, access control, and non-repudiation.
3. It must be confirmed that requests for modifications to electronic communications services come from the subscriber or are made with the subscriber's consent.
4. Guarantee non-repudiation of processing.
5. Guarantee traceability of look-ups and in operation processing activity.
6. Restrict employee information access to that information which is necessary for the employee concerned to carry out his or her duties, and to the time during which such access is necessary.

7. Information compilation due to customer service and invoicing shall be separated from the compilation of information on electronic communications traffic that can be used for investigation of criminal cases and for public safety; for example, the contents of electronic communications.
8. Maintain an uninterrupted path of evidence that could be used to investigate security events. Pre-configure equipment and define processing in such a manner that as many important instances of this sort appear clearly in monitoring systems.
9. Maintain and review regularly documents of access authorisations and access rights. Access controls in electronic communications equipment shall be configured in accordance with the information in the documents.
10. Appropriate measures must be adopted so as to guarantee end-to-end information security in communications under the following circumstances:

a. Employees are engaged in remote access and teleworking on sensitive electronic communications systems.
b. Electronic communications undertaking grant their customers special remote access to the customer's systems via the electronic communications undertaking access control and communications network, such as access to corporate mailboxes or data storages from a cell phone.

CHAPTER IV
Miscellaneous provisions

Article 13
Outsourcing of electronic communications network operations

An electronic communications undertaking is authorised to negotiate with a third party for the operation, in whole or in part, of the electronic communications network. Administrative responsibility and risk management may not be outsourced, however. The requirement for such an agreement, however, is that the electronic communications undertaking must verify that the party in question has set an information security policy and can carry out internal controls and can adopt the necessary security measures as set forth in this Regulation. A written contractual agreement shall be concluded in order to guarantee this. The agreement shall, among other things:

1. Provide for the hosting party's obligation to work in accordance with the instructions of the electronic communications undertaking and the provisions contained in this Regulation.
2. Contain a description of the service to be rendered and specify the level of service requested. It shall also describe the steps that shall be taken if the service does not fulfil these provisions.
3. Contain a provision concerning confidentiality, which shall guarantee compliance with the pertinent provisions of the Electronic Communications Act.
4. Guarantee that the electronic communications undertaking is entitled to monitor the operations to which the agreement applies.
5. Guarantee that the Post and Telecom Administration has access to information from the hosting party and that the Administration can, in the interest of supervision, examined the hosting party's premises.

Article 14

Protection of connections at the network termination point

Electronic communications undertakings shall carry out and maintain connections at the network termination point with security in mind and shall, among other things, take the following measures:

1. When an electronic communications undertaking provides connections and equipment that are utilised jointly with other customers, the undertaking shall separate their traffic in such a way that customers cannot monitor each other's traffic.
2. The undertaking shall disconnect customers, or their services, from the electronic communications network if their connection substantially jeopardises information safety and electronic communications network availability. The disconnection and reconnection shall be carried out in accordance with pre-determined procedures and instructions given by the electronic communications undertaking. In carrying this out, it is permissible to consider special circumstances, such as the type of connection involved.

Article 15

Information on security risks and security incidents

Customers must be notified of any security incidents that cause disturbance to continuous electronic communications services, if confidentiality on a specific network or customer information is seriously jeopardised due to a security risk on electronic communications networks.

Electronic communications undertakings shall have clear and effective procedures for such notifications. 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.

If the measures that electronic communications undertakings adopt in their electronic communications networks do not apply to a specific security incident, the undertakings shall advise their customers concerning measures to counteract vulnerabilities that could result in further spread of the security incident into their systems; for example, to recommend a special software or cryptographic technology for use in public IP networks, including the Internet.

In order to enhance the integrity and security of electronic communications networks in Iceland, the Post and Telecom Administration may decide that specified data concerning information security or suspicious incidents on electronic communications networks must be submitted to security teams that operate in accordance with Article 25 of the Regulation on Protection, Functionality, and Quality of IP Electronic Communications Services, no. 1223/2007.

Article 16

Access to information

Electronic communications undertakings shall submit to the Post and Telecom Administration or its representative all information concerning the organisation of their information security matters, including security policy, risk assessment, business continuity plans, description of security measures, and internal controlling reports, whenever the Administration requests such information. Furthermore, the Administration may request further explanations and data concerning specific security incidents that can occur in electronic communications operations.

Article 17

Testing and audits

The Post and Telecom Administration is authorised to test the security of information in electronic communications networks and conduct audits of whether electronic communications undertakings are in compliance with these Regulation. It may carry out such testing and audits on its own initiative or in response to a submitted comment. Testing applies to public 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 18

Entry into force

These Rules shall take effect on 1 July 2008.

Article 19

Authority

The Post and Telecom Administration has issued this Regulation on the Functionality of Public Communications Networks (SIC), 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