



Regulation

ON INFORMATION SECURITY AND FUNCTIONALITY OF INTERNET ACCESS SERVICES

Issued in Helsinki on 18 September 2008

The Finnish Communications Regulatory Authority (FICORA) has, under sections 19 and 20 of the Act on the Protection of Privacy in Electronic Communications of 16 June 2004 (516/2004) and section 129 of the Communications Market Act of 23 May 2003 (393/2003), prescribed as follows:

Section 1 Scope of application

This Regulation applies to the production of Internet access services provided in public communications networks, and to systems, communications networks and services used by a telecommunications operator to provide these services.

Section 2 Definitions

In this Regulation, "customer subscription" means logical interface between a customer network and the Internet, intended to be used both by consumers and companies.

In this Regulation, "customer subscription services" mean services that a telecommunications operator provides to its customers via the customer subscription for transferring Internet traffic.

In this Regulation, "transit traffic" or "transit service" means service that a telecommunications operator provides to its customers or another operator for the purpose of exchanging or transferring Internet traffic.

In this Regulation, "filtering" means prevention or restriction of Internet traffic in accordance with predetermined rules.

Section 3

Information security in customer subscriptions

A telecommunications operator must perform the implementation and maintenance of customer subscriptions in such a manner that information security aspects are taken into consideration.

When a telecommunications operator provides a customer subscription with shared capacity among other subscribers, it must separate the subscribers' traffic in such a manner that subscribers cannot unlawfully monitor each others' traffic. An operator must ensure that unauthorized redirection of another subscriber's traffic between subscriptions is impossible.

Prior to connecting the customer subscription, a telecommunications operator must inform the customer of general information security risks and subscription type-specific risks, and of methods available for ensuring information security.

A telecommunications operator must define and describe to the customer the essential technical restrictions affecting the use of the customer subscription. These restrictions may, for example, relate to communication ports, protocols or traffic volume and they may be permanent or specific for the subscription type. The description must also include the actions to be taken in case the subscription or services are used in an exceptional manner.

Section 4

Directing and routing of e-mail traffic to a consumer subscription

A telecommunications operator providing Internet connections must prevent incoming SMTP (Simple Mail Transfer Protocol) traffic to a consumer subscription from elsewhere than via agreed servers intended for SMTP traffic.

Notwithstanding the provisions of subsection 1, a telecommunications operator may allow incoming SMTP traffic to the subscriber connection from elsewhere than via the agreed servers intended for SMTP traffic. In this case,

an operator must inform the subscriber of the risks related to open communications.

Section 5

Directing and routing of outgoing e-mail traffic from a consumer subscription

A telecommunications operator providing Internet connections must prevent unrestricted outgoing SMTP traffic from consumer subscriptions otherwise than via agreed servers intended for outgoing SMTP traffic.

Notwithstanding the provisions of subsection 1, a telecommunications operator may allow unrestricted outgoing SMTP traffic even otherwise than via the agreed servers intended for outgoing SMTP traffic. In this case, an operator must inform the subscriber of the risks related to open communications and particularly monitor the volume of outgoing SMTP traffic from the subscriber connection in its communications network. An operator must also be prepared to react to disruptions rapidly.

Section 6

Address-based filtering in customer subscriptions

A telecommunications operator must filter outgoing traffic from a customer subscription to a communications network in cases where the source address is not assigned to this particular customer subscription.

An operator must perform the filtering in a network element closest to the customer interface and where it is technically most feasible.

Section 7

Detection and filtering of malicious traffic in customer subscriptions

A telecommunications operator must monitor and, when necessary, resolve the events in its communications network in order to detect traffic that endangers the information security or usability of a communications network or communications service.

A telecommunications operator must have processes and operations models for temporary filtering of customer subscription traffic in situations which endanger the information security or usability of a communications network or communications service.

A telecommunications operator must disconnect a customer subscription or its service from the public communications network, if a subscription essentially endangers the information security or usability of a communications service. Disconnection and reconnection of a subscription must be carried out in accordance with the predefined processes and guidelines of the operator. Special circumstances due to the subscription type may be taken into consideration when the measures are implemented.

Section 8

Information security of a backbone network

A telecommunications operator must have internal instructions and operations models for denial-of-service attacks and other events that may endanger the information security or usability of a communications network or communications service.

A telecommunications operator must be prepared to take action in order to restrict traffic related to denial-of-service attacks and to trace traffic with incorrect source addresses.

Section 9

Address and route filtering in a backbone network

Telecommunications operators must, in their mutual interconnection traffic, prevent the transmission of such traffic where source address is not in the route advertising of the transferring operator.

Routes belonging to a telecommunications operator's networks must be filtered from received route advertising, unless otherwise agreed about a specific network.

A telecommunications operator must filter such incoming traffic to its own communications network where the source address has been assigned to this particular operator, unless otherwise agreed about the transmission of such traffic.

A telecommunications operator must prevent, at network interfaces, the transfer of broadcast messages intended for network elements connected to the public Internet.

A telecommunications operator must document the use of addresses assigned to it, and which it advertises, by registering the networks with a public Internet Routing Registry.

A telecommunications operator that provides transit services must ensure that the customer networks it advertises are registered with a public Internet Routing Registry.

When a telecommunications operator uses filtering rules based on address spaces reserved for special purposes or unused addresses spaces for the purpose of filtering traffic or routes, it must ensure that the filtering rules are up-to-date.

Section 10

Detection and filtering of malicious traffic in a backbone network

A telecommunications operator must monitor and, where necessary, resolve the events in its backbone network in order to detect traffic that may endanger the information security or usability of a communications network or communications service.

Section 11

Monitoring of functionality and quality of Internet access services

A telecommunications operator must continuously monitor the quality and reliability of the Internet access services. Telecommunications operators must monitor and compile statistics at least of the following:

- Significant exceptional situations affecting the usability of communications networks or services
- network load
- interruptions in the Internet access service sorted by type
- faults found in individual customer subscriptions sorted by type
- number of subscriptions disconnected on the basis of this Regulation.

Section 12

Operator's contact information in public IP address registers

A telecommunications operator must see to that the WHOIS database of the Regional Internet Registry (RIR), who assigned the IP address block, contains relevant contact information regarding address spaces allocated to the operator or operator's customers, abuse information included.

FICORA 13 A/2008 M

A telecommunications operator must see to that the contacts made on the basis of the abuse information with parties responsible for the management of address spaces in the possession of the operator or operator's customers are registered, and that the contacts are regularly monitored.

Section 13
Entry into force

This Regulation enters into force on 1 November 2008 and will remain in force until further notice. The Regulation repeals FICORA's regulation FICORA 13/2005 M of 3 November 2005 on the information security and functionality of Internet access services.

Section 14

Information and publication

This Regulation is included in the Series of Regulations issued by the Finnish Communications Regulatory Authority and it can be obtained from the FICORA Customer Service Office:

Office address	Itämerenkatu 3 A, HELSINKI
Postal address	P.O. Box 313 FI-00181 HELSINKI
Tel. national	09 6966 500
Tel. international	+358 9 6966 500
Fax national	09 6966 410
Fax international	+358 9 6966 410
Website	http://www.ficora.fi/
Business ID	0709019-2

Helsinki 18 September 2008

Director-General

Rauni Hagman

Director

Timo Lehtimäki