Issued:	Entry into force:	Validity:
[dd/mm/yyyy]	[dd/mm/yyyy]	until further notice

Legal basis:
Act on Electronic Communications Services (917/2014), sections 244, 247 and 272

Provisions on sanctions for operations violating this Regulation are laid down in:
Act on Electronic Communications Services (917/2014), sections 330–332, 340 and 349

Implemented EU legislation:
Directive (EU) 2018/1972 of the European Parliament and of the Council, Article 40
Directive 2002/58/EC of the European Parliament and of the Council, Article 4

Modification details:
Repeals Regulation 67 A/2015 M on information security in telecommunications operations issued by the Finnish Communications Regulatory Authority (FICORA) on 4 March 2015

Regulation on information security in telecommunications operations

Table of contents

Chapter 1 Scope of application and definitions

1 Scope of application

1. This Regulation applies to public telecommunications services.

2. Subsection 1 of section 15 of the Regulation is also applied to a public authority network and a communications service related to public authority communications insofar as they are interconnected to a public communications network or a publicly available communications service.

3. The Regulation covers the following:
   - Chapter 2: information security measures in all public communications networks and commonly available communications services;
   - Chapter 3: specific information security requirements for interfaces;
   - Chapter 4: specific requirements for internet access services;
   - Chapter 5: specific requirements for text and multimedia message services; and
   - Chapter 6: specific requirements for email services.

2 Definitions

1. For the purposes of this Regulation:

   1) *customer interface* means an interface through which the communications network, terminal or application of a customer of the telecommunications operator is connected to a public communications network;

   2) *open mail relay* means an email relay system that a third party is able to use for relaying email messages without authorisation;

   3) *malicious traffic* means electronic messages (a) that jeopardise the information security of communications networks or services connected to them as well as information systems, (b) at which actions may be targeted in the manner referred to in section 272, subsection 1, paragraph 2 of the Act on Electronic Communications Services in order to safeguard the possibilities of the sender or recipient of the message for communications, or (c) that are used to prepare for payment fraud referred to in Chapter 37, section 11 of the Criminal Code to be implemented on a wide scale via communications services;

   4) *filtering* means preventing or limiting malicious traffic, removing malicious software that poses a threat to information security from electronic messages, or other comparable technical measures, including tagging the messages as malicious traffic;

   5) *email service* means the transfer, transmission or reception service of electronic mail messages that uses internet name services in the transmission of messages;

   6) *communications network or service component* means a network element, device or information system of which the communications network or service is comprised, or which it uses;

   7) *interconnection interface* means a connection interface between telecommunications operators' communications networks or services;

   8) *text messaging service* means a short message transmission service via a short messaging service centre of the mobile network; and

9) *multimedia message service* means a service for transmitting short messages that contain multimedia objects, such as images, sound, video and edited text via the multimedia message service centre of the mobile network.

2. In addition, this Regulation uses the definitions laid down in section 3 of the Act on Electronic Communications Services (917/2014).

Chapter 2 General information security requirements

3 Consideration of information security issues

1. The telecommunications operator must take the following into consideration in the different life cycle stages of communications networks and services:

   1) information security and risk management;

   2) personnel security;

   3) information system and telecommunications security as well as physical security;

   4) information secure operations and change management;

   5) detection and management of information security incidents and threats;

   6) continuity management;

   7) monitoring, testing and information security assessments; and

   8) maintaining threat awareness and providing information to users and subscribers.

2. The telecommunications operator must document and maintain an up-to-date description on how it will implement the factors in accordance with subsection 1 as well as the other requirements mentioned later in this Chapter in its activities.

4 Information security and risk management

1. Telecommunications operators must take the management of information security and risks into account by implementing the following requirements at a minimum:

   1) The telecommunications operator must have an appropriate information security policy and its specifying measures that it must maintain regularly, taking account of at least the changes in the operating environment, the incidents detected, exercises and predictable changes to the information security threat environment.

   2) The telecommunications operator must identify the functions, data and systems that are critical to the continuity of its telecommunications operations as well as evaluate and address as a continuous process any information security risks to which they may be exposed. Special attention must be paid to the risk assessment of supply chains, virtualisation environments and edge computing units.

   3) The telecommunications operator must specify the appropriate information security roles and responsibilities in accordance with the information security policy and the operating principles that specify it. The telecommunications operator must prevent the creation of combinations of responsibilities and tasks that endanger information security, or if this is not possible, manage the risks due to them in other ways.

4) The telecommunications operator must specify appropriate information security requirements that apply to supplier relationships and supplier agreements, and draw up specifying measures and risk management processes which ensure the information security of communications networks and services throughout the supply chain.

2. The results of the risk management process in subsection 1, item 2 above must be kept for at least three years or for the three most recent risk treatments, whichever storage period is the longest.

5 Personnel security

The telecommunications operator must take personnel security into account by implementing the following requirements at a minimum:

1) The telecommunications operator must perform the appropriate checks in order to ensure the reliability of their personnel, if this is necessary with regard to the duties and responsibilities of the person.

2) The telecommunications operator must ensure that the personnel have sufficient information security skills and that information security training is organised regularly to maintain the competence of the personnel. The telecommunications operator must ensure that its personnel are aware of the information security policy and operating principles referred to in section 4.1.1 of the Regulation as well as their goals and impact on their own duties.

3) The telecommunications operator must have appropriate procedures for managing the information security risks due to changes occurring in the personnel or their duties.

4) The telecommunications operator must have appropriate procedures for addressing security incidents due to the actions of the personnel involving compliance with the operating principles and procedures on information security and in order to process information security breaches due to the actions of the personnel.

6 Information system and telecommunications security as well as physical security

1. The telecommunications operator must take the information system and telecommunications security into account by implementing the following requirements at a minimum:

1) Appropriate procedures must be used to manage access to the communications network and information systems of the telecommunications operator as well as access rights management; they are maintained in accordance with the targeted operating principles concerning access management.

2) The telecommunications operator must ensure the integrity of the communications networks and services, the terminals used by the personnel and the information systems, and protect them from insertion of malicious code as well as from malware that could change the functions of the systems.

3) The telecommunications operator must protect the systems critical to the communications networks and services from denial-of-service attacks. The protective measures must be scaled in accordance with an up-to-date risk assessment.

4) The telecommunications operator must have targeted operating principles and appropriate procedures concerning the use of cryptography and encryption during the storage and transfer of traffic data, messages, location data, control traffic and the information material of the telecommunications operator used in telecommunications operations. With regard to information security risks, the operating principles must define at least the information material and traffic cases that require encryption as well as the encryption methods and practices used, the management of encryption keys and exceptions to the use of encryption. The telecommunications operator must use an appropriate encryption whenever it is technically possible and proportionate with regard to the information security risks related to the storage or transfer of data and the costs incurred due to the encryption.

5) The telecommunications operator must have appropriate operating principles and procedures for the protection and management of encryption key materials and secret information used for authentication.

6) The communications network and service components implemented in a virtualisation environment must be implemented so that only the functionalities and access rights necessary to their operation are permitted.

2. The telecommunications operator must have appropriate operating principles and procedures for ensuring the physical safety of information systems, devices, data and premises and the environmental conditions of devices. Provisions on the physical protection of equipment facilities are also found in the Regulation of the Finnish Transport and Communications Agency on resilience of communications networks and services and of synchronisation of communications networks.

7 Information secure operation and change management

1. The telecommunications operator must implement the operation and change management of communications networks and services so that they take the following requirements into account at a minimum:

   1) The telecommunications operator must have appropriate operating principles and procedures for the use of the communications network or service components (operation).

   2) The telecommunications operator must have appropriate change management procedures that reduce the likelihood of information security incidents caused by the changes or restore the status before the change or some other functional status, if necessary.

   3) The telecommunications operator must have appropriate operating principles and procedures for asset and configuration management.

2. Provisions on change management can also be found in section 9 of the Regulation of the Finnish Transport and Communications Agency on disturbances in telecommunications services.

8 Testing and information security assessments

The telecommunications operator must implement the information security testing and assessment of communications networks and services so that they take account of at least the following requirements:

1) The telecommunications operator must have appropriate operating principles and procedures for testing the information security of the communications network and service components and, if necessary, carrying out security assessments on them based on a risk assessment.

2) The telecommunications operator must have appropriate operating principles and procedures for monitoring the realisation of its information security policy, operating principles and the information security requirements of its operations (information security assessment). The results of at least the latest assessment must be stored.

9 Maintaining threat information

The telecommunications operator must have appropriate procedures for collecting threat information related to the information security of communications networks and services and assessing the threats.

10 Compliance with standards

1. The mobile network telecommunications operator must have appropriate procedures that ensure the implementation of the security requirements of the technical specifications (standards) referred to in Annex 1 in the fourth-generation mobile network implemented by using LTE technology, the fifth-generation mobile network as well as the IP-based public telephone service. The latest version of the standard approved by 3GPP must be used that corresponds to the functionality implemented by the telecommunications operator in its communications network or service.

2. The telecommunications operator may decide not to implement a security requirement referred to in subsection 1 if implementing it is not appropriate for the purpose, taking account of its significance to the information security of the communications network or service in the case in question as well as the other related measures to ensure information security.

3. The telecommunications operator must maintain a description of how it takes subsection 1 into account in its operations. Not implementing the security function or mechanism under subsection 2 and the grounds for the non-implementation must be documented separately for each security requirement.

11 Information material

The telecommunications operator must have in place a classification system for any information material that is important for the telecommunications operations, classification criteria, and processing procedures for information material associated with the classification.

12 Identifying the customer to ensure information security

The telecommunications operator must have appropriate operating principles and procedures that are sufficiently reliable with regard to the risk level of the transaction for identifying the user or subscriber before essential changes affecting the information security of the communications service are made to the customer's service or confidential information is disclosed to the user or subscriber.

13 Documentation of IP addresses

The telecommunications operator must ensure that the IP addresses assigned to it and advertised by it are appropriately documented in the database of the IP address registry that allocated the address space or other appropriate IP address registry.

14 Management network and management connection traffic

1. The telecommunications operator must have appropriate operating principles and procedures on network management and management connections.

2. The telecommunications operator must protect and, if necessary, encrypt the management traffic of the communications network or service components appropriately so that making unauthorised changes to the communications network or service components is prevented in accordance with the operating principles.

3. The telecommunications operator must have appropriate procedures for assessing the information security threats caused by the terminal devices used for network management and managing the risks caused by them.

Chapter 3 Specific requirements for the interfaces of communications networks and services

15 Prevention of and protection from interference in interfaces

1. The telecommunications operator must ensure that its communications network or service components will not cause interference to other communications networks or services. The telecommunications operator must have appropriate mechanisms in place for preventing such interference.

2. The telecommunications operator must protect its communications network and services from malicious traffic from interconnection, application and customer interfaces by applying the required protection mechanisms to its networks.

16 Shutting down unnecessary ports, services and protocols

The telecommunications operator must ensure that no unnecessary services or protocols are enabled in the components or the associated ports of communications networks or services in the operator's interconnection or customer interfaces.

17 Protecting IP interconnection interfaces and filtering the traffic

1. In order to protect IP interconnection interfaces, the telecommunications operator must do at least the following:

   1) detect routing deviations;

   2) protect sessions used to exchange routing information whenever possible;

   3) filter traffic containing an incorrect IP source address towards its communications network, including traffic, in which the source address of a received IP package

      i) belongs to an IP address space managed or advertised by the telecommunications operator itself or belongs to a private IP address space; or

ii) does not belong to the routes advertised to other telecommunications operators by a telecommunications operator that delivers traffic;

4) from the route advertisements received, reject

i) route advertisements belonging to the operator's own address blocks or to those provided by the telecommunications operator to one of its customers and that cannot be expected to be advertised by other telecommunications operators; and

ii) route advertisements with an incorrect ROA (Route Origin Authorisation); and

5) create ROAs for the IP prefixes it manages, if this is technically possible, and ensure that they are signed and published.

2. The traffic defined in subsection 1, item 3 above may nevertheless be forwarded and the route advertisements described in item 4 may be allowed for individual networks, if a separate agreement has been made on the matter between the operators.

18 Preventing the falsification of IP addresses (IP spoofing) in the customer interface

1. The telecommunications operator must filter any traffic from a customer interface to the communications network with a source address that is not assigned to the customer interface in question. The telecommunications operator must apply filtering in the network element that is closest to the customer interface and in which it is technically the most appropriate to apply the filtering.

2. As a milder alternative to the traffic filtering referred to above in subsection 1, the customer may be contacted for the purpose of solving the situation that poses a threat to information security.

19 Protecting the interfaces of the mobile network

The telecommunications operator must protect the interfaces of the mobile network to ensure the information security of the communications network and service and prevent the unauthorised traffic re-routing. In its mobile network interfaces the telecommunications operator must, at a minimum:

1) monitor the information security of signalling interfaces and design, implement and maintain information security management measures of the signalling interface based on up-to-date threat information and risk assessment;

2) protect the mobile network slice management connection so that only authorised parties can create, change or remove slices or receive information on the features, subscribers or users of the slice;

3) in addition to the primary authentication of the mobile network, implement a slice-specific terminal device access right authentication and authorisation using identification information other than that used in the primary authentication, if it is necessary considering the information security threats related to the use of the slice and the technical possibilities of implementing access right authentication and authorisation; and

4) protect the communications network and communications services from any malicious traffic that the edge computing unit may target at them by implementing the necessary protection mechanisms in the network.

Chapter 4 Specific requirements for internet access services

20 Separation of traffic in internet access services

1. The telecommunications operator must separate the traffic of its customers, ensuring that the users of various subscriber connections cannot have unauthorised access to each other's traffic. The telecommunications operator must ensure that an unauthorised re-routing of traffic between subscriber connections is not possible.

2. Notwithstanding the provisions of subsection 1, the telecommunications operator may provide unencrypted WLAN connections without traffic separation at the radio interface.

21 Directing of outgoing email traffic from consumer subscriber connections

1. The telecommunications operator must prevent unlimited outbound SMTP traffic from consumer subscriber connections other than through servers intended for outgoing SMTP traffic.

2. Notwithstanding the provisions of subsection 1, the telecommunications operator may allow unlimited SMTP traffic not going through servers intended for outgoing SMTP traffic. In this case, the telecommunications operator must inform the subscriber about the risks associated with open traffic. The telecommunications operator must also be able to react quickly in case of interference.

22 Obligation to filter malicious traffic in an internet connection service

1. The telecommunications operator must have appropriate systems and procedures for temporarily filtering out malicious traffic from the internet connection service.

2. The telecommunications operator must regularly assess the suitability of its filtering measures for their purpose and ensure that the filtering rules are up to date.

3. The telecommunications operator must maintain up-to-date documentation on the filtering measures it applies.

23 Disconnection of an internet access service connection

1. The telecommunications operator must disconnect a customer connection from the communications network, if the information security of the communications service is materially compromised due to traffic to or from the connection, and the measures set out in section 22 of this Regulation or other less severe measures are inadequate for ensuring the information security of the communications service.

2. Disconnecting and reconnecting must follow the processes and guidelines defined in advance by the telecommunications operator. In applying the measures, the particular circumstances arising from the type of subscriber connection and the severity of the information security threat may be taken into account.

Chapter 5 Specific requirements for text and multimedia message services

24 Filtering text and multimedia message traffic

1. The telecommunications operator must have appropriate systems and procedures for temporarily filtering out malicious traffic in text and multimedia messaging services.

2. The telecommunications operator offering text and multimedia messaging services must:

   1) tag or filter out from incoming message traffic any traffic identified as malicious, unless specifically otherwise agreed with the customer; and

   2) filter out from outgoing message traffic any traffic identified as malicious.

3. The provisions of subsections 1 and 2 above do not apply to a multimedia messaging service, if the telecommunications operator otherwise detects disturbances that endanger information security and it has the ability to react quickly to them.

4. The telecommunications operator must regularly assess the suitability of its filtering measures for their purpose and ensure that the filtering rules are up to date.

Chapter 6 Specific requirements for email services

25 Contact information for email services and address resource management

1. The telecommunications operator providing email services must ensure that the domains used in connection with the provision of email services include "postmaster" and "abuse" email addresses or other abuse contact information and that messages sent to these addresses are regularly monitored.

2. The telecommunications operator providing email services must not transfer an email address released from a customer to another customer before a period of six months has passed since the release of that email address.

26 Specific obligation to filter email services

1. The telecommunications operator providing email services must have in place up-to-date and reliable mechanisms for identifying and processing malicious email traffic.

2. The telecommunications operator providing email services must:

   1) filter out any incoming malicious traffic that compromises the information security of systems employed to provide email services;

   2) tag or filter out from incoming email traffic any traffic identified as malicious, unless specifically otherwise agreed with the customer; and

   3) filter out from outgoing email traffic any traffic identified as malicious.

27 Open relays for email

The telecommunications operator providing email services must ensure that the email systems administered by it will not function as open mail relays.

28 Connection between customer and email server

1. The telecommunications operator providing email services must offer its customers as the primary alternative a secure connection between the customer and the electronic mailbox and between the customer and the outgoing email server. In the secure connection, the user of the service must be authenticated and the traffic must be encrypted. The obligation also applies to other than browser-based email services.

2. Customer connections of browser-based email services must be secured.

Chapter 7 Provisions on entry into force

29 Entry into force [and transition period]

1. [This Regulation enters into force three months after the Regulation is issued]

2. This Regulation repeals Regulation 67 A/2015 M on information security in telecommunications operations issued by the Finnish Communications Regulatory Authority (FICORA) on 4 March 2015.

In Helsinki on (DD) Month 20(YY)

Party making the decision

Presenting officer

Annex 1 Applicable technical standards

3GPP TS 33.116, Security Assurance Specification (SCAS) for the MME network product class

3GPP TS 33.216, Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class

3GPP TS 33.226, Security assurance for IP Multimedia Subsystem (IMS)

3GPP TS 33.250, Security assurance specification for the PGW network product class

3GPP TS 33.326, Security Assurance Specification (SCAS) for the Network Slice-Specific Authentication and Authorization Function (NSSAAF) network product class

3GPP TS 33.511, Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class

3GPP TS 33.512, 5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)

3GPP TS 33.513, 5G Security Assurance Specification (SCAS); User Plane Function (UPF)

3GPP TS 33.514, 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class

3GPP TS 33.515, 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class

3GPP TS 33.516, 5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class

3GPP TS 33.517, 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class

3GPP TS 33.518, 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class

3GPP TS 33.519, 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class

3GPP TS 33.520, 5G Security Assurance Specification (SCAS); Non-3GPP InterWorking Function (N3IWF)

3GPP TS 33.521, 5G Security Assurance Specification (SCAS); Network Data Analytics Function (NWDAF)

3GPP TS 33.522, 5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP)

3GPP TS 33.523, 5G Security Assurance Specification (SCAS); Split gNB product classes

3GPP TS 33.526, Security Assurance Specification for Management Function (MnF)

3GPP TS 33.527, Security Assurance Specification (SCAS) for 3GPP virtualized network products

3GPP TS 33.528, Security Assurance Specification (SCAS) for Policy Control Function (PCF)

3GPP TS 33.529, Security Assurance Specification (SCAS) for the Short Message Service Function (SMSF) network product class

3GPP TS 33.537, Security Assurance Specification (SCAS) for the Authentication and Key Management for Applications (AKMA) Anchor Function (AAnF)

[Out of the above, standards at their preparation stage will be included in this Annex, if they are published within the schedule of the Regulation.]