This document contains draft Regulations setting out security measures to be taken by providers of public electronic communications networks and services. It has been made available by the Department of Digital, Culture, Media and Sport to illustrate how the powers in the Telecommunications (Security) Bill (as introduced to Parliament) may be used, and to support early engagement with providers.

STATUTORY INSTRUMENTS

2021 No.

ELECTRONIC COMMUNICATIONS

The Electronic Communications (Security Measures) Regulations 2021

Made - - - -	***
Laid before Parliament	***
Coming into force - -	***

CONTENTS

The Secretary of State, in exercise of the powers conferred by section 105B and 105D of the Communications Act 2003(**a**), makes the following Regulations.

Citation and commencement

1. These Regulations may be cited as the Electronic Communications (Security Measures) Regulations 2021 and come into force on [date].

Interpretation

2. In these Regulations—

"the Act" means the Communications Act 2003;

(**a**) 2003 c.21: section 105B is inserted by section 1 of the Telecommunications (Security) Act 2021 (c. *); section 105D is inserted by section 2 of that Act.

"content", in relation to a signal, means any element of the signal, or any data attached to or logically associated with the signal, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but—

(a) any meaning arising from the fact of the signal or from any data relating to the transmission of the signal is to be disregarded, and

(b) anything which is systems data as defined by section 263(4) of the Investigatory Powers Act 2016(**a**) is not content;

"external signal", in relation to a public electronic communications network, means any signal transmitted by or to the network;

"network provider" means a person who provides a public electronic communications network;

"privileged access", in relation to a public electronic communications network or a public electronic communications service, means direct access to security critical functions of the network or service (and includes any access capable of making material changes to security critical functions);

"security critical function", in relation to a public electronic communications network or a public electronic communications service, means any function of the network or service whose operation is likely to have a material impact on the proper functioning of the entire network or service or a material part of it, including its structure, separation, confidentiality, integrity or availability; and includes any function of the network or service whose operation is likely to have a material impact on the proper functioning of a security critical function;

"security permission", in relation to a public electronic communications network or a public electronic communications service, means a permission given to a person in relation to the network or service that would increase the person's opportunity to cause a security compromise to occur in relation to the network or service;

"security risk", in relation to a public electronic communications network or a public electronic communications service, means the extent of the overall security risk to the network or service as determined by an assessment under regulation 9(2)(c);

"sensitive data", in relation to a public electronic communications network or a public electronic communications service, means—

(a) data which defines, controls or materially contributes to a security critical function,

(b) data which is the content of a signal, or

(c) other data which would produce or enable a material security compromise if it were to be compromised;

"service provider" means a person who provides a public electronic communications service;

"signal" has the same meaning as in section 32 of the Act.

Network architecture

3.—(1) A network provider must—

(a) except in relation to an existing part of the public electronic communications network, design, construct and maintain the network in a manner which appropriately reduces the risks of security compromises,

(b) in relation to an existing part of the public electronic communications network, redesign and reconstruct that part, so far as is appropriate and proportionate, in a manner which appropriately reduces those risks, and

(c) maintain the public electronic communications network in a manner which appropriately reduces those risks.

(**a**) 2016 c. 25.

(2) For the purposes of paragraph (1), any part of a public electronic communications network is an "existing part" if it was brought into operation before the coming into force of these Regulations.

(3) The duty in paragraph (1) includes in particular a duty—

(a) to identify, record and reduce the risks of security compromises to which the entire network and each particular function, or type of function, of the network may be exposed, taking into account—

(i) whether the function contains sensitive data,

(ii) whether the function is a security critical function,

(iii) the physical location of the function or data related to the function,

(iv) the exposure of the function to external signals, and

(v) any other relevant factor,

(b) to identify and record the extent to which the network is exposed to external signals,

(c) to ensure appropriate network separation of each part of the network, particularly between security critical functions and other functions of the network, and between equipment and software used for separate security critical functions,

(d) to design, construct and maintain the network to ensure that security critical functions are located in an appropriate place and appropriately protected,

(e) to take appropriate measures in the procurement, configuration, management and testing of equipment to ensure the security of the equipment and functions carried out on the equipment, and

(f) to ensure that the network provider is able to assess risks to, and where necessary maintain the operation of, a public electronic communications network located in the United Kingdom, without reliance on persons, equipment or stored data located outside the United Kingdom.

(4) In paragraph (3)(c), "network separation", in relation to a public electronic communications network, means the separation of particular data transmitted by means of the network from other data transmitted by means of the network—

(a) as a result of the physical properties of the network (physical separation), or

(b) as a result of the use in relation to those data of functions that are different from those used in relation to other data (logical separation).

Protection of data and network functions

4.—(1) A network provider must use technical means—

(a) to protect any data stored by electronic means in a manner which is proportionate to the sensitivity of the data, and

(b) to protect functions of the public electronic communications network in a manner which is proportionate to the sensitivity of each function.

(2) A service provider must use technical means—

(a) to protect any data stored by electronic means in a manner which is proportionate to the sensitivity of the data, and

(b) to protect the functions of the public electronic communications network by means of which the public electronic communications service is provided, in a manner which is proportionate to the sensitivity of each function.

(3) The duties in paragraphs (1) and (2) include in particular duties to—

(a) ensure that workstations through which privileged access is possible are not exposed to external networks,

(b) monitor and reduce the risks of security compromises arising out of external signals,

(c) ensure the security of security critical functions, including the security of their location,

(d) provide a high level of protection to sensitive data held by the network or service,

(e) ensure that any equipment supplied to customers which is used or intended to be used as part of the network or service is secure, and

(f) ensure that tools enabling monitoring or audit cannot be accessed from outside the United Kingdom if they enable monitoring or audit—

(i) in real time, or

(ii) of the content of signals.

(4) A network provider must use within the public electronic communications network signals which, by encryption or otherwise, reduce the risks of security compromises.

(5) A service provider must—

(a) monitor and reduce the risks of security compromises relating to subscribers' SIM cards occurring in relation to the public electronic communications network by means of which the public electronic communications service is provided, and

(b) replace SIM cards in cases where it is appropriate to do so in order to reduce such risks.

(6) In paragraph (5), "SIM card" means a subscriber identity module or other hardware storage device intended to store an International Mobile Subscriber Identity (IMSI) and associated cryptographic material, and the reference to replacing a SIM card includes a reference to the application to a SIM card of any process which permanently replaces one IMSI and associated cryptographic material with another.

Monitoring and audit

5.—(1) A network provider must take proportionate measures—

(a) to monitor and analyse signals entering, transiting or leaving the electronic communications network for the purpose of identifying anomalous activity, and

(b) to investigate anomalous activity.

(2) A network provider or service provider must monitor, analyse and audit the use of the public electronic communications network or public electronic communications service for the purpose of identifying the occurrence of any security compromise, using automated means of monitoring and analysis where possible.

(3) The duty in paragraph (2) includes in particular a duty—

(a) to maintain a record of all access to the network or service (but not of the content of signals),

(b) to have in place means and procedures for producing immediate alerts of all manual amendments to security critical functions,

(c) to analyse promptly all activity relating to security critical functions of the network for anomalous activity,

(d) to ensure that all data required for the purposes of a duty under paragraph (1) or sub-paragraphs (a) to (c) is held securely for at least 13 months,

(e) to take measures to prevent activities that unreasonably restrict monitoring, analysis and investigation under this regulation,

(f) where appropriate, to share information about anomalous activities with other network providers or service providers, using automatic means so far as possible,

(g) to record the type, location, software and hardware information and identifying information of equipment supplied by them which is used or intended to be used as part of the network, and

(h) to avoid dependence on persons, equipment or stored data located outside the United Kingdom to monitor and audit the use of networks located in the United Kingdom.

(4) This regulation does not require or authorise the monitoring of transmissions in such a way as to make any content of a signal available, at any time while it is being transmitted or while stored in or by the public electronic communications network or public electronic communications service (whether before or after its transmission), to a person who is not the sender or intended recipient of the signal.

Supply chain

6.—(1) A network provider or service provider must identify and reduce the risks of security compromises occurring as a result of the provider depending on other persons ("third party suppliers") to supply, provide or make available goods, services or facilities for use in connection with the provision of the public electronic communications network or public electronic communications service.

(2) A network provider or service provider ("the primary provider") must take appropriate measures—

(a) to understand and address the risks of security compromises arising out of the supply chain, including—

(i) those arising during the formation, existence and termination of contracts with third party suppliers, and

(ii) those arising from the supply chains of third party suppliers,

(b) to ensure, through contractual arrangements and other measures, that third party suppliers—

(i) take appropriate measures to identify, disclose to the primary provider and reduce the risks of, security compromises to the primary provider's network or service arising from the use of their products and services,

(ii) where the third party supplier is itself a network provider and is given access to the primary provider's network or to sensitive data, take measures for the purposes mentioned in section 105A(1) of the Act equivalent to those that the primary provider is required to take in relation to the primary provider's network,

(iii) take appropriate measures to enable the primary provider to monitor all activity undertaken by the third party supplier on the primary provider's network,

(iv) take appropriate measures to co-operate with the primary provider in the resolution of incidents which cause or contribute to a security compromise or a potential security compromise to the primary provider's network or service, and

(v) take appropriate measures to require those who, in relation to them, are themselves third party suppliers to observe equivalent policies and procedures in relation to the risks of security compromises and their reduction,

(c) to ensure that all network connections and data sharing with third party suppliers are managed securely,

(d) to have appropriate written plans to manage the termination of, and transition from, contracts with third party suppliers whilst maintaining the security of the network or service, and

(e) to reduce dependence on a single third party supplier in the procurement of any equipment in any part of the network that connects directly to customers or performs the associated transmission functions.

(3) A network provider must—

(a) ensure that there is in place at all times a written plan to maintain the normal operation of the public electronic communications network in the event that supply or support from a third party supplier is interrupted, and

(b) review that plan on a regular basis.

Prevention of security compromise and management of security permissions

7.—(1) A network provider or service provider must take such measures as are appropriate and proportionate to prevent the occurrence of security compromises in relation to the public electronic communications network or public electronic communications service.

(2) The duty in paragraph (1) includes in particular a duty—

(a) to exercise control over network management functions at all times,

(b) to require two or more independent credentials to be present in order to access security critical functions,

(c) to ensure the security of security critical functions, including the security of means of access to them,

(d) to avoid using default credentials wherever possible, in particular by avoiding, to the extent possible, using devices and services with default credentials that cannot be changed,

(e) where, despite sub-paragraph (d), default credentials have been used, to assume for the purposes of assessing the risks of security compromises that any such default credentials are publicly available,

(f) to ensure that data that could be used to cause a security compromise in relation to the network or service (whether or not stored by electronic means) is stored securely,

(g) to carry out changes to operations of security critical functions through automated functions where possible,

(h) to ensure that material or manual changes to the operations of the security critical functions proposed by a user are approved by another suitably competent and authorised person before the change occurs,

(i) to undertake regular reviews of their security measures, taking into account relevant developments relating to the risks of security compromises occurring,

(j) to have the ability to respond to the occurrence of a security compromise within a reasonable period appropriate to the security risk of the provider and the size of the provider's undertaking, and

(k) to take proportionate measures to deploy appropriate and effective patches or mitigation relating to risks of security compromises (including software updates and equipment replacement)—

(i) within the 14 days beginning with the day on which the patch or mitigation becomes available, or

(ii) within such longer period as may be determined by the provider on reasonable grounds to be appropriate, having regard to the severity of the risk of security compromise which the patch or mitigation addresses, and recorded by the provider in writing.

(3) A network provider must have in place, and use where appropriate, means and procedures for isolating security critical functions from all signals which the provider does not believe on reasonable grounds to be safe.

(4) A network provider or service provider must limit, so far as is consistent with the maintenance and operation of the public electronic communications network or the provision of the public electronic communications service, the number of persons given security permissions and the extent of any security permissions given.

(5) A network provider or service provider must also—

(a) ensure that passwords and credentials are managed, stored and assigned securely,

(b) take all proportionate measures to ensure that each user or system accessing security critical functions uses a credential which identifies them individually,

(c) take appropriate measures, including the avoidance of common credential creation processes, for the purpose of ensuring that credentials are unique and not capable of being anticipated by others,

(d) keep records of all third parties that are able to access the public electronic communications network or public electronic communications service, and the nature of that access,

(e) limit the extent of a user's access to security critical functions to that which is strictly necessary to enable the user to undertake the activities which the provider authorises the user to carry on, and

(f) take into account the user's location when determining their security permission.

Remediation and recovery

8.—(1) A network provider or service provider must take such measures as are appropriate and proportionate for the purposes of limiting the adverse effects of security compromises and enabling the provider to recover from any security compromises.

(2) The duty in paragraph (1) includes in particular a duty—

(a) to acquire, and retain within the United Kingdom—

(i) offline and online copies of information necessary to operate security critical functions of the public electronic communications network or public electronic communications service, and

(ii) an online copy, and so far as is proportionate an offline copy, of information necessary to operate functions of the public electronic communications network or public electronic communications service other than security critical functions,

(b) to replace copies held for the purpose of sub-paragraph (a) with reasonable frequency, proportionate to the security risk of the network provider or service provider and the size of the provider's undertaking,

(c) to have means and procedures in place for—

(i) promptly identifying the occurrence of any security compromise,

(ii) responding to the occurrence of a security compromise within a reasonable period appropriate to the security risk of the network provider or service provider and the size of the provider's undertaking,

(iii) responding to any unauthorised access to or control over security critical functions by taking action as soon as reasonably possible, in a way that does not create an unreasonable risk of the occurrence of a further security compromise in relation to the network or service, to ensure that only authorised users have access to the network or service, and

(iv) replacing information damaged by security compromises with the information contained in the copy referred to in sub-paragraph (a).

Governance and accountability

9.—(1) A network provider or service provider must ensure appropriate management of persons given responsibility for the taking of measures on behalf of the provider for the purposes mentioned in section 105A(1) of the Act.

(2) The duty in paragraph (1) includes in particular a duty—

(a) to treat security as an essential business function and give a person or committee at board level (or equivalent) responsibility for ensuring effective security management, including through the promulgation of clear security policies and appropriate resourcing,

(b) to identify and take all proportionate measures to reduce the risks of security compromises arising through unauthorised conduct by persons involved in the provision of the public electronic communications network or public electronic communications service, including measures involving the consideration of the susceptibility of those persons to improper influence, whether by reason of their country of residence or otherwise,

(c) to undertake at least once in any period of 12 months a review of the risks of security compromises to the network or service in order to produce a written assessment of the extent of the overall risk of security compromises occurring, taking into account—

(i) in the case of a network provider, the risks identified under regulation 3(3)(a) and (b),

(ii) the risks identified under regulation 6(2)(a),

(iii) the results of the reviews carried out pursuant to regulation 7(2)(i),

(iv) any risks identified under sub-paragraph (b), and

(v) any other relevant information,

(d) to establish and regularly review business procedures relating to the risk of security compromise, including procedures to manage security incidents at varying levels of severity,

(e) to ensure that their business procedures set out clearly established roles and responsibilities and channels for communicating and escalating risks and issues, including in the context of incident reporting,

(f) to ensure that their business procedures include a post-incident review process in relation to all security incidents and that the procedure involves consideration of the outcome of the review at an appropriate governance level and the use of that outcome to inform the security of future products and services, and

(g) to have a standardised way of categorising and managing security incidents.

(3) A network provider must identify and prioritise necessary network security updates and network equipment upgrades and, where these are not implemented within a reasonable period appropriate to the security risk of the network provider and the size of the network provider's undertaking, the network provider must arrange for the level of risk arising from non-implementation to be discussed and recorded at an appropriate governance level.

Competency

10.—(1) A network provider or service provider must ensure that persons given responsibility for the taking of measures on behalf of the provider for the purposes mentioned in section 105A(1) of the Act ("the responsible persons") and the persons who support the operation of security critical functions—

(a) are competent to discharge that responsibility or to support the operation of those functions, and

(b) are given appropriate powers and resources to enable them to do so.

(2) The duty in paragraph (1) includes in particular a duty—

(a) to ensure that the responsible persons have appropriate knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the operation of security critical functions,

(b) to ensure that persons who support the operation of security critical functions are appropriately trained in security measures,

(c) to ensure that the responsible persons are competent to enable the provider to carry out monitoring and auditing duties under regulation 5 of the network provider or service provider, and are given appropriate resources for that purpose,

(d) to ensure that the responsible persons are competent to show appropriate understanding and appraisal of the activities and recommendations of third party suppliers and are given appropriate resources for that purpose, and

(e) to ensure that new equipment is set up according to a secure configuration approved by appropriately trained security personnel, following business processes which are able to demonstrate that the configuration has been carried out in this way, and to record any variance which falls below the vendor's minimum security recommendations.

(3) In paragraph (2)(d), "third party supplier" has the same meaning as in regulation 6.

Testing

11.—(1) A network provider or service provider must carry out, or arrange for another person to carry out, such tests in relation to the network or service as are appropriate and proportionate for the purpose of assessing the resilience of the network or service to the risks of security compromises occurring.

(2) The tests must involve simulating, so far as is possible, techniques that might be expected to be used by a person seeking to cause a security compromise.

(3) The network provider or service provider must ensure, so far as is reasonably practicable—

(a) that the manner in which the tests are to be carried out is not made known to the persons involved in identifying and responding to security compromises in relation to the network or service or the persons supplying any equipment to be tested, and

(b) that measures are taken to prevent any of those persons being able to anticipate the tests to be carried out.

(4) The references to tests in relation to the network or service include references to—

(a) tests in relation to premises used in connection with the provision of the network or service, and

(b) tests in relation to persons involved in the provision of the network or service.

Assistance

12.—(1) A service provider—

(a) must not do anything which impedes the taking by the relevant network provider of a measure required by these Regulations or the efficacy of a measure so required, and

(b) must, when requested by the relevant network provider, provide the relevant network provider with such assistance as is proportionate in the taking of any measure required by these Regulations.

(2) In paragraph (1) "the relevant network provider", in relation to a service provider, means the person providing the public electronic communications network by means of which the service is provided.

(3) A network provider or service provider must, so far as is proportionate, share information about any security compromise relating to the public electronic communications network or public electronic communications service with any other network provider or service provider in relation to whose public electronic communications network or public electronic communications service the security compromise may cause a connected security compromise.

(4) The information to be shared under paragraph (3) may be shared subject to reasonable and appropriate controls for the purposes of security, genuine commercial interest, or to secure

compliance with the data protection legislation, as defined by section 3 of the Data Protection Act 2018(**a**).

(5) A network provider or service provider must seek appropriate assistance from other persons where necessary to reduce the risk of security compromises to the provider's public electronic communications network or public electronic communications service.

(6) In paragraph (3) "connected security compromise" has the same meaning as in section 105A of the Act(**b**).

Signatory text

Name
Address — Parliamentary Under Secretary of State
Date — Department

EXPLANATORY NOTE

(This note is not part of the Regulations)

These Regulations require the providers of public electronic communications networks and public electronic communications services to take certain security measures.

(**a**) 2018 c. 12.
(**b**) Section 105A is inserted by section 1 of the Telecommunications (Security) Act 2021 (c. *);