Jersey

DRAFT TELECOMMUNICATIONS (SECURITY MEASURES) (JERSEY) ORDER 202-

Contents

Article

Jersey

DRAFT TELECOMMUNICATIONS (SECURITY MEASURES) (JERSEY) ORDER 202-

Made	*[date to be inserted]*
Coming into force	*[date to be inserted]*

THE MINISTER FOR SUSTAINABLE ECONOMIC DEVELOPMENT makes this Order under Articles 24L and 24N of the Telecommunications (Jersey) Law 2002 –

1 Interpretation

In this Order –

"assessed security risk", in relation to a public electronic communications network or a public electronic communications service, means the overall risk of a security compromise occurring in relation to the network or service, as determined by an assessment under Article 11(b);

"connected security compromise" has the meaning given in Article 24K(4) of the Law;

"content", in relation to a signal, means any element of the signal, or any data attached to or logically associated with the signal, that reveals anything that 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 that is systems data is not content;

"incoming signal", in relation to a public electronic communications network, means a signal received by the network;

"Law" means the Telecommunications (Jersey) Law 2002;

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

"public electronic communications network" has the meaning given in Article 24A of the Law;

"public electronic communications service" has the meaning given in Article 24A of the Law;

"responsible person" means a person given responsibility for taking measures on behalf of the network provider or service provider for the purposes mentioned in Article 24K(1) of the Law;

"security compromise" has the meaning given in Article 24K(2) of the Law;

"security critical function", in relation to a public electronic communications network or a public electronic communications service, means a function of the network or service whose operation is likely to have a material impact on the proper operation of the entire network or service or a material part of it;

"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 gives the person an opportunity to cause a security compromise in relation to the network or service;

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

(a) data that controls, or significantly contributes to, a security critical function; or

(b) data that is the content of a signal;

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

"systems data" means data that is connected to enabling or facilitating any of the following –

(a) a telecommunication system (including any apparatus forming part of the system);

(b) a telecommunication service provided by means of a telecommunication system;

(c) a system on which communications or other information are held on or by means of the system (a "relevant system"), including any apparatus that forms part of the system;

(d) a service provided by means of a relevant system;

"third-party supplier", in relation to a network provider or service provider, means a person who supplies, provides or makes available goods, services or facilities for use in connection with the provision of the public electronic communications network or public electronic communications service.

2 Application of this Order

This Order applies only to the network providers and service providers listed in Schedule 1.

3 Network architecture

(1) A network provider must take appropriate and proportionate measures to ensure –

(a) except in relation to an existing part of its public electronic communications network, that the network is designed and constructed in a way that reduces the risks of a security compromise occurring;

(b) in relation to an existing part of its public electronic communications network, that the part is redesigned and developed in a way that reduces the risks of a security compromise occurring; and

(c) that its public electronic communications network is maintained in a way that reduces the risks of a security compromise occurring.

(2) An existing part of a public electronic communications network is a part that was brought into operation before the commencement of this Order.

(3) The duty in paragraph (1) includes a duty to –

(a) identify and reduce the risks of a security compromise to which the network as a whole, and each particular function or type of function of the network, may be exposed, giving consideration to –

(i) whether the function contains sensitive data;

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

(iii) the location of the equipment performing the function or storing data related to the function; and

(iv) the exposure of the function to incoming signals;

(b) make a written record, at least once in any 12-month period, of the risks identified under sub-paragraph (a);

(c) identify and record the extent to which the network is exposed to incoming signals;

(d) design and construct the network in a way that ensures that security critical functions are appropriately protected and that the equipment performing those functions is appropriately located;

(e) take appropriate and proportionate 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) take appropriate and proportionate measures to ensure that the network provider –

(i) is able, without reliance on persons, equipment or stored data located outside of the British Islands, to identify the risks of a security compromise occurring;

(ii) is able to identify any risk that it may become necessary to operate the network without reliance on persons, equipment or stored data located outside of the British Islands; and

(iii) if it should become necessary to do so, would be able to operate the network without reliance on persons, equipment or stored data located outside of the British Islands.

(4) A network provider must retain a record made under paragraph (3)(b) or (c) for at least 3 years.

(5) A network provider or service provider must take appropriate and proportionate measures to ensure that its public electronic communications network or public electronic communications service is designed so that a security compromise in relation to part of the network or service does not affect other parts of the network or service.

4 Protection of data and network functions

(1) A network provider must use appropriate and proportionate technical means to –

(a) protect data that is stored by electronic means and relates to the operation of its public electronic communications network, in a way that is appropriate to that data; and

(b) protect functions of its public electronic communications network in a way that is appropriate to those functions.

(2) A service provider must use appropriate and proportionate technical means to –

(a) protect data that is stored by electronic means and relates to the operation of its public electronic communications network, in a way that is appropriate to that data; and

(b) protect functions of the public electronic communications network used to provide the public electronic communications service, to the extent that those functions are under the control of the service provider, in a way that is appropriate to those functions.

(3) In paragraphs (1) and (2), "protect" means protect from anything involving a risk of a security compromise occurring in relation to the public electronic communications network or public electronic communications service in question.

(4) The duties in paragraphs (1) and (2) include duties to take appropriate and proportionate measures –

(a) to ensure that workstations through which it is possible to make significant changes to security critical functions are not exposed –

(i) if, in the case of a public electronic communications network, the workstation is directly connected to the network, to signals that are incoming signals in relation to the network;

(ii) if, in the case of a public electronic communications service, the workstation is directly connected to the public electronic communications network through which the service is provided, to signals that are incoming signals in relation to that network; or

(iii) if, in either case, the workstation is operated remotely, to signals other than those that the workstation must be capable of receiving in order to enable changes to security critical functions authorised by the network provider or service provider to be made;

(b) to monitor and reduce the risks of a security compromise occurring as a result of incoming signals received in the network or in a network that is used to provide the service; and

(c) to monitor and reduce the risks of a security compromise occurring as a result of the characteristics of any equipment supplied to customers that is used or intended to be used as part of the network or service.

(5) A network provider must use within its public electronic communications network signals that, by encryption, reduce the risks of a security compromise occurring.

(6) A service provider must –

(a) monitor and reduce the risks of a security compromise relating to customers' SIM cards occurring in relation to the public electronic communications network used to provide the public electronic communications service; and

(b) replace SIM cards if it is appropriate to do so in order to reduce the risks.

(7) In paragraph (6), "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 applying to a SIM card any process that permanently replaces an IMSI and associated cryptographic material with another.

5 Protection of certain tools enabling monitoring or analysis

(1) This Article applies in relation to a public electronic communications network or public electronic communications service if the network or service includes tools that enable –

(a) the monitoring or analysis in real time of the use or operation of the network or service; or

(b) the monitoring or analysis of the content of signals.

(2) If the tools are stored on equipment located outside of the British Islands, the network provider or service provider must take measures to identify and reduce the risks of a security compromise occurring as a result of the tools being stored on equipment located outside of the British Islands.

(3) The network provider or service provider must ensure that the tools –

(a) are not capable of being accessed from a country listed in Schedule 2; and

(b) are not stored on equipment located in any of those countries.

6 Monitoring and analysis

(1) A network provider must take appropriate and proportionate measures to monitor and analyse access to security critical functions of its public electronic communications network for the purpose of identifying anomalous activity that may involve a risk of a security compromise occurring.

(2) A network provider or service provider must take appropriate and proportionate measures to –

(a) monitor and analyse the operation of security critical functions of its public electronic communications network or public electronic communications service for the purpose of identifying the occurrence of a security compromise, using automated means of monitoring and analysis where possible; and

(b) investigate any anomalous activity in relation to the network or service.

(3) The duty in paragraph (2) includes a duty to –

(a) maintain a record of all access to security critical functions of the network or service, including the persons obtaining access;

(b) identify and record all cases where a person's access to security critical functions of the network or service exceeds the person's security permission;

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

(d) analyse promptly all activity relating to security critical functions of the network or service for the purpose of identifying anomalous activity;

(e) 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; and

(f) take measures to prevent activities that would restrict the monitoring and analysis required by this Article.

(4) A network provider or service provider must record the type, location, software and hardware information and identifying information of equipment supplied by the network provider or service provider that is used or intended to be used as part of its public electronic communications network or public electronic communications service.

7 Supply chain

(1) A network provider or service provider must take appropriate and proportionate measures to identify and reduce the risks of a security compromise occurring in relation to its public electronic communications network or public electronic communications service as a result of an act by a third-party supplier.

(2) The risks referred to in paragraph (1) include –

(a) those arising during the formation, existence or termination of contracts with third-party suppliers; and

(b) those arising from third-party suppliers with whom the network provider or service provider has a contractual relationship contracting with other persons for the supply, provision or making available of any goods, services or facilities for use in connection with the provision of its public electronic communications network or public electronic communications service.

(3) A network provider or service provider (the "primary provider") must take appropriate and proportionate measures to –

(a) ensure, by means of contractual arrangements, that each third-party supplier –

(i) takes appropriate measures to –

(A) identify the risks of a security compromise occurring in relation to the primary provider's network or service as a result of the primary provider's use of goods, services or facilities supplied, provided or made available by the third-party supplier;

(B) disclose those risks to the primary provider; and

(C) reduce those risks;

(ii) if the third-party supplier is a network provider and is given access to the primary provider's network or service or to sensitive data, takes appropriate measures for the purposes mentioned in Article 24K(1) of the Law, in relation to goods, services or facilities supplied, provided or made available by the third-party supplier to the primary provider, that are equivalent to the measures that the primary provider is required to take in relation to the primary provider's network or service;

(iii) takes appropriate measures to enable the primary provider to monitor all activity undertaken or arranged by the third-party supplier in relation to the primary provider's network or service; and

(iv) takes appropriate measures to co-operate with the primary provider in the resolution of an incident that causes or contributes to the occurrence of a security compromise in relation to the primary provider's network or service or of an increased risk of a compromise occurring;

(b) ensure that all network connections and data sharing with third-party suppliers, or arranged by third-party suppliers, are managed securely; and

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

(4) A network provider must –

(a) ensure that there is in place at all times a written plan to maintain the normal operation of its public electronic communications network in the event that the supply, provision or making available of goods, services or facilities by a third-party supplier is interrupted; and

(b) review that plan on a regular basis and amend it if required by the review.

8 Prevention of unauthorised access or interference

(1) A network provider or service provider must take appropriate and proportionate measures to reduce the risks of the occurrence of a security compromise that consists of unauthorised access to its public electronic communications network or public electronic communications service.

(2) The duty in paragraph (1) includes a duty –

(a) to ensure that responsible persons have an appropriate understanding of the operation of the network or service;

(b) to require multi-factor authentication for access to an account capable of making changes to security critical functions;

(c) to ensure that significant or manual changes to security critical functions must, before the change is made, be proposed by 1 person authorised by the network provider or service provider in question and approved by another person from among the responsible persons;

(d) to avoid the use of default credentials wherever possible, in particular by avoiding, as far as possible, the use of devices and services with default credentials that cannot be changed;

(e) if, despite sub-paragraph (d), default credentials have been used, to assume, for the purpose of identifying the risks of a security compromise occurring, that those default credentials are publicly available;

(f) to ensure that information that could be used to obtain unauthorised access to the network or service (whether or not stored by electronic means) is stored securely; and

(g) to carry out changes to security critical functions through automated functions where possible.

(3) A network provider must have in place, and use where appropriate, means and procedures for isolating security critical functions from signals that the provider does not reasonably believe are safe.

(4) A network provider or service provider must limit, so far as is consistent with the maintenance and operation of its public electronic communications network or the provision of its 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 –

(i) managed, stored and assigned securely; and

(ii) revoked when no longer needed;

(b) take appropriate and proportionate measures to ensure that each user or system authorised to access security critical functions uses a credential that identifies them individually when accessing those functions;

(c) take appropriate and proportionate measures, including the avoidance of common credential creation processes, to ensure that credentials are unique and not capable of being anticipated by others;

(d) keep records of all persons who –

(i) in the case of a network provider, have access to its public electronic communications network other than merely as end-users of a public electronic communications service provided by means of the network; and

(ii) in the case of a service provider, have access to its public electronic communications service other than merely as end-users of the service; and

(e) limit the extent of the access to security critical functions given to a person who uses the network or service to that which is strictly necessary to enable the person to undertake the activities that the provider authorises the person to carry on.

(6) A network provider or service provider must ensure that –

(a) no security permission is given to a person while the person is in a country listed in Schedule 2; and

(b) a security permission cannot be exercised while the person to whom it is given is in in a country listed in Schedule 2.

9 Preparing for remediation and recovery

(1) A network provider or service provider must take appropriate and proportionate measures to prepare for the occurrence of a security compromise, with a view to limiting the adverse effects of any security compromise and enabling the provider to recover from a security compromise.

(2) The duty in paragraph (1) includes a duty –

(a) to create or acquire, for the purposes mentioned in that paragraph, and to retain –

(i) within the British Islands, an online copy of information necessary to maintain the normal operation of its public electronic communications network or public electronic communications service; and

(ii) in Jersey, an offline copy of that information so far as is proportionate;

(b) to replace, with the most recent version, copies held for the purpose of sub-paragraph (a) with reasonable frequency, appropriate to the assessed security risk of its network or service; and

(c) to have the means and procedures in place –

(i) for promptly identifying the occurrence of a security compromise and assessing its severity, impact and likely cause;

(ii) for promptly identifying any mitigating actions required as a result of the occurrence of a security compromise;

(iii) if the occurrence of a security compromise gives rise to the risk of a connected security compromise, for preventing the transmission of signals that give rise to that risk;

(iv) for dealing with the occurrence of a security compromise within a reasonable period appropriate to the assessed security risk of the network provider or service provider, and without creating any risk of a further security compromise occurring;

(v) for ensuring that, if the network provider or service provider is unable to take steps to prevent any adverse effects (on the network or service

or otherwise) arising from the occurrence of a security compromise within the period of 14 days beginning with the day on which it occurs, the network provider or service provider is able to prepare a written plan as to how and when they will take those steps;

(vi) for dealing with any unauthorised access to, or control over, security critical functions by taking action as soon as reasonably possible, and without creating a risk of a further security compromise occurring, to ensure that only authorised users have access to the network or service; and

(vii) for replacing information damaged by a security compromise with the information contained in the copy referred to in sub-paragraph (a).

(3) For the purposes of paragraph (2)(a) –

(a) an "online copy" is a copy that is held on the public electronic communications network or public electronic communications service in question; and

(b) an "offline copy" is a copy that is stored in a way that ensures it is not exposed to signals conveyed by means of the network or service in question.

10 Governance

(1) A network provider or service provider must ensure appropriate and proportionate management of responsible persons.

(2) The duty in paragraph (1) includes a duty to –

(a) establish, and regularly review, the provider's policy as to measures to be taken for the purposes mentioned in Article 24K(1) of the Law;

(b) ensure that the policy includes procedures for the management of security incidents, at varying levels of severity;

(c) have a standardised way of categorising and managing security incidents;

(d) ensure that the policy provides channels through which risks identified by persons involved at any level in the provision of the network or service are reported to persons at an appropriate governance level;

(e) ensure that the policy provides for a post-incident review procedure in relation to security incidents and that the procedure involves consideration of –

(i) the outcome of the review at an appropriate governance level; and

(ii) the use of that outcome to inform future policy; and

(f) give a person or committee at board level (or equivalent) responsibility for –

(i) supervising the implementation of the policy; and

(ii) ensuring the effective management of responsible persons.

(3) In paragraph, (2) "security incident" means an incident involving –

(a) the occurrence of a security compromise; or

(b) an increased risk of a security compromise occurring.

(4) A network provider or service provider must take appropriate and proportionate measures to identify and reduce the risks of a security compromise occurring as a result of unauthorised conduct by persons involved in the provision of the public electronic communications network or public electronic communications service.

11 Reviews

A network provider or service provider must –

(a) undertake regular reviews of the provider's security measures in relation to its public electronic communications network or public electronic communications service, taking into account relevant developments relating to the risks of a security compromise occurring; and

(b) undertake at least once in any 12-month period a review of the risks of a security compromise occurring in relation to the network or service and produce a written assessment of the extent of the overall risk of a security compromise occurring within the next 12 months, taking into account –

(i) in the case of a network provider, risks identified under Article 3(3)(a);

(ii) risks identified under Article 5(2);

(iii) risks identified under Article 6(1);

(iv) risks identified under Article 7(1);

(v) risks identified under Article 10(4);

(vi) the results of reviews carried out under sub-paragraph (a);

(vii) the results of tests carried out under Article 14; and

(viii) any other relevant information.

12 Patches and updates

A network provider or service provider must –

(a) if the person providing software or equipment used for the purposes of the public electronic communications network or public electronic communications service makes available a patch or mitigation relating to the risk of a security compromise occurring (including software updates and equipment replacement), take appropriate and proportionate measures to deploy the patch or mitigation within an appropriate period, giving consideration to the severity of the risk of security compromise that the patch or mitigation addresses;

(b) identify any need for a security update or equipment upgrade and implement the necessary update or upgrade within an appropriate period, giving consideration to the assessed security risk of the network provider or service provider; and

(c) arrange for a decision to be taken, at an appropriate governance level and recorded in writing, as to what period the network provider or service provider considers appropriate –

(i) for the purposes of sub-paragraph (a), if the network provider or service provider considers in relation to a particular patch or mitigation that an appropriate period is more than 14 days beginning with the day on which the patch or mitigation becomes available; or

(ii) for the purposes of sub-paragraph (b), if there is a significant risk of a security compromise occurring.

13 Competency

(1) A network provider or service provider must take appropriate and proportionate measures to ensure that responsible persons –

(a) are competent to discharge their responsibility; and

(b) are given sufficient resources to enable them to do so.

(2) The duty in paragraph (1) includes a duty to take appropriate and proportionate measures –

(a) to ensure that the responsible persons have appropriate knowledge and skills to perform their responsibilities effectively;

(b) to ensure that the responsible persons are competent to enable the network provider or service provider to perform the provider's duties under Article 6, and are given sufficient resources for that purpose;

(c) to ensure that the responsible persons –

(i) are competent to show appropriate understanding and appraisal of the activities of third-party suppliers and of any recommendations made by third-party suppliers for the purposes of identifying and reducing the risks of a security compromise occurring; and

(ii) are given sufficient resources for that purpose; and

(d) if new equipment is supplied, provided or made available by a third-party supplier –

(i) to ensure that the equipment is set up according to a secure configuration approved by appropriately trained security personnel, following procedures that enable it to be demonstrated that the configuration has been carried out in that way; and

(ii) to record any failure to meet recommendations of the third-party supplier as to the measures that are essential to reduce the risks of a security compromise occurring as a result of the way in which the equipment is set up.

14 Testing

(1) A network provider or service provider must, at appropriate intervals, carry out, or arrange for a suitable person to carry out, tests in relation to the network or service that are appropriate and proportionate for the purpose of identifying the risks of a security compromise occurring in relation to its public electronic communications network or public electronic communications service.

(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 way in which the tests are to be carried out is not made known to –

(i) the persons involved in identifying and responding to the risks of a security compromise occurring in relation to the network or service; or

(ii) the persons supplying any equipment to be tested; and

(b) that measures are taken to prevent the persons mentioned in sub-paragraph (a) 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 tests in relation to –

(a) the competence and skills of persons involved in the provision of the network or service; and

(b) the possibility of unauthorised access to places where the network provider or service provider keeps equipment used for the purposes of the network or service.

15 Assistance

(1) A network provider or service provider (the "relevant provider") must, so far as is appropriate and proportionate, provide information about a security compromise to another network provider or service provider if –

(a) the security compromise occurs in relation to the relevant provider's public electronic communications network or public electronic communications service; and

(b) it appears to the relevant provider that the security compromise may cause a connected security compromise in relation to the other network or service.

(2) Information provided under paragraph (1) that relates to a particular business must not, without the consent of the person carrying on the business –

(a) be used or disclosed by the recipient, except for the purposes of –

(i) identifying or reducing the risks of a security compromise occurring in relation to the recipient's network or service; or

(ii) preventing or mitigating the adverse effects of a security compromise that has occurred in relation to the recipient's network or service; or

(b) be retained by the recipient any longer than is necessary for those purposes.

(3) A network provider ("network provider A") must, when requested by a service provider or another network provider ("network provider B"), give network provider B assistance that is appropriate and proportionate in the taking by network provider B of a measure required by this Order in relation to anything that –

(a) has occurred in relation to network provider A's public electronic communications network;

(b) is a security compromise in relation to that network; and

(c) could cause a connected security compromise in relation to network provider B's public electronic communications network or public electronic communications service.

(4) A service provider ("service provider A") must, when requested by a network provider or another service provider ("service provider B"), give service provider B assistance that is appropriate and proportionate in the taking by service provider B of any measure required by this Order in relation to anything that –

(a) has occurred in relation to service provider A's public electronic communications service;

(b) is a security compromise in relation to that service; and

(c) could cause a connected security compromise in relation to service provider B's public electronic communications network or public electronic communications service.

(5) A network provider or service provider must, if necessary to reduce the risks of a security compromise occurring in relation to the provider's public electronic communications network or public electronic communications service, request another person to give any assistance that paragraph (3) or (4) requires the other person to give.

16 Citation and commencement

This Order may be cited as the Telecommunications (Security Measures) (Jersey) Order 202- and comes into force immediately after Regulation 8 of the Telecommunications Law (Jersey) Amendment Regulations 2024 comes into force.

SCHEDULE 1

(Article 2)

NETWORK PROVIDERS AND SERVICE PROVIDERS TO WHICH THIS ORDER APPLIES

Home Net Limited, a company incorporated in the Bailiwick of Jersey under registered number 67490 and with its registered office at Bramble Bank, Le Vieux Beaumont, St. Peter, Jersey, JE3 7EA;

JT (Jersey) Limited, a company incorporated in the Bailiwick of Jersey under registered number 83487 and with its registered office at No. 1 The Forum, Grenville Street, St. Helier, Jersey, JE4 8PB;

Newtel Limited, a company incorporated in the Bailiwick of Jersey under registered number 70523 and with its registered office at Unit 2B, Centenary House, La Grande Route de St. Pierre, St. Peter, Jersey, JE3 7AY;

Sure (Jersey) Limited, a company incorporated in the Bailiwick of Jersey under registered number 84645 and with its registered office at The Powerhouse, Queen's Road, St. Helier, Jersey JE2 3AP.

SCHEDULE 2

(Articles 5(3) and 8(6))

COUNTRIES LISTED FOR PURPOSES OF ARTICLES 5(3) AND 8(6)

Iran (Islamic Republic of Iran)
North Korea
People's Republic of China
Russia (Russian Federation)