STATES OF JERSEY

DRAFT CYBER SECURITY (JERSEY) LAW 202-

Lodged au Greffe on 24th November 2025
by the Minister for Sustainable Economic Development
Earliest date for debate: 20th January 2026

STATES GREFFE

Jersey

DRAFT CYBER SECURITY (JERSEY) LAW 202-

European Convention on Human Rights

In accordance with the provisions of Article 16 of the Human Rights (Jersey) Law 2000, the Minister for Sustainable Economic Development has made the following statement –

In the view of the Minister for Sustainable Economic Development, the provisions of the Draft Cyber Security (Jersey) Law 202- are compatible with the Convention Rights.

Signed: **Deputy K.F. Morel of St. John, St. Lawrence and Trinity**

Minister for Sustainable Economic Development

Dated: 21st November 2025

REPORT

Executive Summary

Cyber attacks and cyber threats stretch beyond national boundaries. Jersey is not immune.

The draft Cyber Security (Jersey) Law 202- establishes a statutory framework to strengthen Jersey's resilience against cyber threats and safeguard critical infrastructure. It introduces the Jersey Cyber Security Centre (JCSC) as the national authority for cyber security, with a Director granted operational independence and clear objectives to prepare for, protect against, and respond to cyber incidents.

The draft Law sets out governance arrangements, including the creation of Technical Advisory Councils (TACs) to provide expert cyber advice, and mandates strategic planning, annual reporting, and adherence to codes of conduct. It empowers the Director to act as the Single Point of Contact (SPOC) and the JCSC as the Computer Security Incident Response Team (CSIRT) for Jersey, ensuring coordination with domestic regulators and international networks.

A key feature is Operator of Essential Services (OES) designation across sectors such as energy, transport, finance, health, water, digital, postal, food, and public administration. OESs are subject to statutory duties to implement proportionate security measures, report significant cyber incidents within 24 hours, and comply with directions issued by the Minister for Sustainable Economic Development. Government services are similarly bound by these obligations.

The Law provides enforcement mechanisms at Ministerial level, including the imposition of civil penalties of up to £10,000 for non-compliance and criminal sanctions for false or misleading information. It also facilitates secure information sharing between the Director, law enforcement representatives, and international partners, while introducing consequential amendments to related legislation (Computer Misuse, Data Protection, Emergency Powers and Planning, Freedom of Information and Telecommunications).

By aligning with international best practice and the European Network and Information Systems (NIS) Directive, this legislation delivers a robust, future-proof framework for cyber security governance, incident response, and critical infrastructure protection in Jersey.

Introduction

The draft Cyber Security (Jersey) Law 202- (the "draft Law") would, if adopted, demonstrate Jersey's commitment to improving the level of cyber security of the Island's network and information systems for the provision of essential services.

The Minister for Sustainable Economic Development (the "Minister") holds the legal responsibility for the Island's national cyber security, supported by the Director of the Jersey Cyber Security Centre (the "Director"). The draft Law establishes the role of the Director and the Jersey Cyber Security Centre (JCSC) as a technical advisory body for cyber security for the Island.

The objectives and functions of the Director are to *prepare for, protect from, defend against and facilitate recovery from, cyber threats or cyber attacks affecting Jersey*.

In addition, the draft Law provides provision for:

- Identification of Jersey's Operators of Essential Services (OESs) and their cyber security duties including the mandatory reporting of significant cyber incidents to JCSC and a duty to implement appropriate and proportionate security measures to identify cyber threats and reduce the risk of cyber incidents;

- Establishment of Technical Advisory Councils (TACs), where expert subject matter advice is sought in respect of cyber security matters affecting Jersey or to help the Director deliver against the Director's responsibilities or functions;
- Fines and penalties, where the Minister has the power to impose a civil financial penalty, to a maximum of £10,000, on an OES for contravention of a provision of the Law. This fine does not extend to contravention by a government service. The penalty for providing false or misleading information applies to all.

Background

The draft law, advances the policy direction and ambition of Jersey's first Cyber Security Strategy, published in 2017, to raise the cyber resilience of the Island. This includes the formation of a cyber incident response capability to support development of trusted cyber threat information sharing and cyber incident reporting mechanisms.

Delivering against the strategy's ambitions, in 2019, the Council of Ministers approved the creation and funding of a Cyber Emergency Response Team (more widely known as a "CERT") as part of the Government Plan (*Cyber Security Growth).* This recommendation was based on a feasibility study conducted in 2018 (originally with Guernsey) to evaluate and identify the core functions that would be required by an operational CERT. This study incorporated significant stakeholder engagement to evaluate an appropriately scaled operational cyber security centre for the Island.

Originally known as the Cyber Emergency Response Team for Jersey (CERT.JE), Jersey's capability was developed with the following remit:

- **Raise Awareness** of cyber security risk and threats by proactively educating businesses and citizens about cyber security threats and steps to mitigate them
- **Provide best practice and guidance** on how businesses should develop incident response plans, cyber security risk assessments and the steps they should be taking to secure their systems and data
- **Active threat intelligence analysis** to prevent, detect and respond to cyber attacks, including providing advice and an incident response capability
- **Incident response capability** to lead and coordinate the response to crisis situations caused by cyber attacks including supporting information sharing, relaying information on steps taken by different organisations to respond to incidents and approaches that have been successful
- **Promote cyber security information sharing** amongst businesses to ensure awareness of existing threats
- **Increase the level of cyber resilience** across the Island, with the collaboration of Government of Jersey, Critical National Infrastructure and business communities to reduce the risk and impact of major cyber incidents
- **Represent Jersey's cyber security interests** within international cyber security bodies and in dealings with other cyber-attack expertise and response centres
- **Uphold Jersey's cyber security reputation** by ensuring Jersey meets the appropriate international standards of best practice for cyber security
- **Appropriate and proportional governance** fiscally responsible to deliver against Government policy

The Department for the Economy (the "Department") recruited the Director of CERT.JE in June 2021 and completed the recruitment of the small technical team in 2022, with no further growth

plans. The Director and the dedicated team will operate at full capacity once the draft Law is enacted, which provides clarity on their mandate and their legal duties and functions.

The latest Island-wide cyber resilience exercise was completed in 2020 and continues to highlight the need on Jersey for specialised cyber security support. This is especially true for the many small, local Jersey businesses who have limited skills and capability to improve their own cyber security posture.

Since November 2021, CERT.JE has operated from separate premises from government and has sought to reassure local businesses experiencing a cyber attack that any sensitive data shared remains independent from government systems, facilitating CERT.JE's ability to raise awareness about potential cyber attacks and provide advice.

The facility was rebranded in late 2021, to become the Jersey Cyber Security Centre (JCSC) to reflect the wider role of the facility - as a technical advisory authority on cyber security on behalf of Jersey, rather than just an emergency cyber response capability.

In developing the draft legislation to reinforce and support JCSC's operations, two public consultations were held, in December 2022/January 2023 and March/April 2024. Feedback was widely sought to help refine the policy intent behind the operational mandate for the Jersey Cyber Security Centre and the cyber security obligations of entities to be captured as Operators of Essential Services (OESs). Input was received from key stakeholders including:

- cyber security businesses on Island;
- regulatory bodies;
- government departments; and
- entities considered critical to the Island's infrastructure.

Engagement continues with entities identified by the draft Law as OESs. Relevant guidance is to be developed and published by JCSC to enable OESs to confidently fulfil their duties under the proposed draft Law.

The Draft Cyber Security (Jersey) Law 202-

The presented draft Cyber Security (Jersey) Law 202- is Jersey's first legislation specifically intended to improve Island-wide cyber resilience. Its objectives are to:

1. Establish a recognised technical cyber security advisory capability for the Island
2. Increase the cyber security of network and information systems and operational technology on which the Island's Operators of Essential Services rely
3. Develop a trusted culture of cyber threat information sharing to mitigate cyber risks and raise cyber resilience

The draft Law reflects global best practice and the minimum legislative cyber security requirements that have been mandated across European member states since 2018[1]. Adoption of the draft Law will reflect Jersey's commitment to being a trusted jurisdiction with which to do business and will enable the proposed Jersey Cyber Security Centre to form deeper collaborative relationships with international cyber security agencies, like the UK National Cyber Security Centre. This will enable Jersey to access wider expert cyber threat and incident information, ultimately raising the resilience of Jersey as a whole.

The proposed objectives and functions of the Director of the Jersey Cyber Security Centre and employees of the JCSC align with those of Cyber Emergency Response Teams (CERTs) in other

[1] See European Directive 2016/1148, "the adoption concerning measure for a high common level of security of network and information systems across the Union": eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:194:FULL

respected jurisdictions, ensuring Jersey's businesses and Islanders have access to local expertise to improve their cyber resilience.

The draft Cyber Security (Jersey) Law 202- is structured as follows:

Part 1: Interpretation This contains the key definitions of words and phrases used within the draft law. Key cyber terms have been defined to ensure a single interpretation. Cyber terms defined include 'cyber attack', 'cyber incident', 'cyber resilience', 'cyber security' and 'cyber threat'.

Part 2: Jersey Cyber Security Centre This Part sets out the establishment of the Jersey Cyber Security Centre (JCSC) as an authority for cyber security in Jersey and creates the role of the Director. The Minister must appoint the Director, with Schedule 1 making further provision with respect to this role.

The Director and employees of the JCSC are all States' employees (Article 2). There is provision for a JCSC code of conduct to be developed and published, that employees of JCSC and the Director must follow. In the event that the JCSC code of conduct is inconsistent with a code of practice issued under the Employment of States of Jersey Employees (Jersey) Law 2005, the States code of practice takes precedence (Article 6).

The Director has the objectives and functions conferred under Part 3 and maintains operational independence, unless directed otherwise through the exercise of the Ministerial powers in Articles 5 and 7. The Director and JCSC must operate independent information and technology systems to securely handle threat and incident information (Article 11).

There are provisions for the optional establishment of one or more Technical Advisory Council (TACs), should the Minister or Director wish to seek advice on matters of cyber security for Jersey or on the Director's own functions and responsibilities (Article 4). Each TAC is to operate under clear terms of reference, to provide clarity about their role, purpose and advice to be provided. Members of TACs are to be appointed by the Minister (Schedule 2), with all TACs convened on a voluntary basis.

Part 2 also specifies the annual governance and funding requirements (Article 10) between the Minister and the Director, to ensure value for money and adherence of expenditure in line with Jersey's public finance legislation. There is a requirement to publish an annual report (Article 8) and a 3-year strategic plan (Article 9). The annual report is to be presented to the Minister and the States Assembly.

There are no provisions within the draft Law for the Director to establish a fee structure to fund the activities of the Jersey Cyber Security Centre.

Part 3: Objectives and Functions of the Director This part defines the objectives, functions and powers of the Director. These are in line with international best practice.

Article 12 sets out the high level objectives of the Director, namely to 'prepare for, protect from, defend against and facilitate recovery from cyber threats or cyber attacks affecting Jersey'.

A cyber attack is considered to affect Jersey if:

- it affects the States of Jersey; a public administration; a government service; a person having a place of business or address in Jersey; an operator of an essential service; (see Part 4); an individual present in Jersey; services using Autonomous System Names and Internet Protocol address prefix assigned to Jersey or for use in Jersey; the .je internet domain; or

- results, or may result in reputational, political, economic or well-being risks to Jersey.

JCSC is to act as Jersey's Single Point of Contact for cyber security (SPOC) (Article 13) to help centralise cyber threat and incident information and communication and to ensure effective international cyber co-operation on behalf of Jersey. JCSC's functions include consulting and co-operating with relevant law enforcement authorities and relevant regulatory bodies.

As the Computer Security Incident Response Team (CSIRT) (Article 14), JCSC must, as far as reasonable practicable, monitor and scan publicly accessible network and information systems to identify malicious activity, configuration errors and vulnerabilities and take the necessary action to resolve them. JCSC also has a function of taking reasonable steps to:

- raise awareness in Jersey of cyber threats, the resulting risks, responses and mitigations;
- understand the current global cyber threat landscape, raising awareness of the threats, resulting risks, responses and mitigations;
- support and co-ordinate the delivery of cyber security services;
- enable and promote cyber security information sharing;
- increase the level of cyber resilience in Jersey; and
- represent Jersey's cyber security interests in international co-operation networks.

Article 15 sets out that the Director may advise the Minister on matters relating to cyber security and that functions are conferred on the Director under this Law or may be conferred on the Director by another enactment.

Article 16 provides the Director the ability to discharge their functions by entering into an agreement with another person. The Director remains responsible for the discharge of the delegated function.

The Director must issue guidance (Article 17) in relation to cyber security and to their functions under Part 3. The Director may seek advice from TACs or other relevant persons to develop the guidance.

In consultation with the Minister, relevant regulatory bodies and Operators of Essential Services, the Director may set or adopt appropriate cyber security standards (Article 18) and must publish guidance in relation to the exercise of their functions.

The Director and employees of JCSC may assist in an investigation (Article 19) into or relating to cyber security if requested by the Information Commissioner, the Jersey Financial Services Commission, the States of Jersey Police Force, the Jersey Competition Regulatory Authority, or another body the Director considers appropriate.

Article 20 details the circumstances in which the Director may provide cyber security services to the States of Guernsey.

Part 4: Operators of Essential Services This part provides for identification of Jersey's Operators of Essential Services. OESs are entities for which a significant cyber incident would pose a reputational, political, economic or wellbeing risk to Jersey. These essential services include entities providing traditional critical infrastructure; sectors who contribute significantly to the overall economy of the Island as well as those services that are pivotal to society.

Schedule 3 captures key Island entities as OESs in the following sectors:

- Electricity (importing, generating, transmitting, selling;

- Crude Oil (importing, storing, delivery, supplying);
- Gas (importing, storing, distributing, selling)
- Sea transport (harbour operations)
- Air transport (airport operations)
- Freight handling (at Jersey ports)
- Road transport and freight distribution (via road to and from Jersey ports)
- Banking
- Medical services (hospital)
- Drinking water (supplying)
- Public communications (telecoms providers)
- Digital services (providing information and communications technology services to other OESs, managed service providers, cloud computing and data centre services based in Jersey)
- Operator of .je domain name (designated manager of the top level domain name, or successor organisation)
- Domain name services (providing registration or DNS services)
- Postal service (Jersey Post International Ltd or subsidiary)
- Courier service (delivery of)
- Couriers of necessary suppliers (supplier of medical supplies)
- Food production (Jersey Dairy)
- Food retail (over 700 square meters or 50% of retail sales area given to sale of food)
- Parishes and public bodies (as specified in Schedule 2 of the Public Finances (Jersey) Law 2019, Jersey regulatory bodies (JFSC, JCRA, JDPA), and Jersey Heritage
- Emergency services (police, ambulance, fire and rescue, airport fire and rescue)

Extensive consultation with proposed OESs has taken place to confirm suitable threshold limits, as detailed in Schedule 3. Engagement will continue with these OESs as relevant guidance is developed by JCSC, to support them in fulfilling their duties under the draft Law. The draft Law requires this guidance to be in place as the draft Law is enacted.

Article 22 provides the detail for designating an Operator of Essential Service provides, with relevant threshold limits detailed in Schedule 3.

The Minister may designate an entity as an OES (Article 22 (5)) and has the power to issue information notices (Article 23) to ensure the Minister has the required information to make such a decision. Provisions are included for the review and revocation of a designation (Article 26) and right of appeal (Article 27).

Article 24 applies, under the specified conditions, if the Minister wishes to designate an OES where the head office is outside Jersey, but considers the service provided is essential to Jersey. Article 25 requires that designated OES to provide details of a person in Jersey authorised to act on their behalf under the Law.

Part 5: Security Duties of Operators of Essential Services For this Part, "government services" (defined as a Minister or an organisational entity that discharges the functions of a Minister) are considered as Operators of Essential Services.

Part 5 details security measures required by identified Operators of Essential Services (OESs) and the notification requirements should they suffer a cyber incident that is considered to have a significant impact on the continuity of the essential service provided. Early notification of such an incident to JCSC enables JCSC to fulfil its objectives to *prepare for, protect from, defend against and facilitate recovery from cyber threats or attacks affecting Jersey.*

OESs are required to take appropriate and proportionate security measures (Article 29) to identify cyber threats; reduce the risk of cyber incidents; prepare for cyber incidents and ensure the continuity of their essential service. They also have a duty to notify the Director of a cyber incident that has, or is likely to have, a significant impact on its cyber resilience or service, within 24 hours of becoming aware (Article 31). The initial report at 24-hours is a high-level report, with information of the significant incident as known at that time. This time period is based on international best practice, as it is widely recognised an early reporting of an incident can help contain it and prevent it affecting other entities or individuals. A quick notification also enables a co-ordinated response and improves cyber security across all sectors.

To support OESs to fulfil their legal obligations, the Director must produce relevant guidance (Article 34), with feedback to be sought from relevant bodies during consultation.

Within Part 5, the Minister has the power to direct OESs to take specified security measures that are appropriate and proportionate to improve their cyber security (Article 30) or in response to a cyber incident (Article 32). In doing so, the Minister must have due regard to the operational independence of OESs (Article 33).

Part 6: Enforcement Details the powers of the Minister to impose a civil financial penalty on an OES to a maximum of £10,000. The Minister does not have the power to fine another Minister or Department or entity defined as a public body, but Article 40 does give the Minister power to direct the "government service" to take the necessary remedial action.

Knowingly providing false or misleading information to the Minister, Director, Jersey Cyber Security Centre or other persons entitled to receive such information is an offence under the draft Law. A person convicted of committing such an offence is liable to imprisonment for 5 years or a fine, or both.

Part 7: Information Sharing and Closing Provisions This Part provides the legal mechanism for entities to share appropriate information with the Director, especially to facilitate information sharing during a cyber incident.

The transitional provisions provide for the current Director and those employed within the JCSC to remain in post.

The States Assembly will have the ability to amend the law by Regulations, except for the following Articles which may be amended by Order:

- Article 8: to amend the provisions required within the published annual report;
- Articles 12(3) and 12(4): to change the definitions of Jersey and external entity affected by a cyber threat or attack;
- Article 15: to make additional or supplementary provision in relation to the functions of the Director; and
- Article 36 (6)(b): to amend the level of financial penalty to be imposed.

The consequential amendments needed to existing Jersey legislation are detailed in Schedule 4. Updates to the Computer Misuse (Jersey) Law 1995 are required to ensure the Director and JCSC can perform their legally mandated functions and to the Emergency

Powers and Planning (Jersey) Law 1990 to widen the remit of the power of the competent authority in relation to telecommunications, to include the cyber security and cyber resilience of Jersey.

Amendments to the Data Protection (Jersey) Law 2018 and the Freedom of Information (Jersey) Law 2011 are with respect to information received in relation to the national security of Jersey. The Minister may provide relevant exemption certificates only for cyber security matters, which is a similar power to that of the Minister for Justice and Home Affairs for all other cases. To date, no certificates have been requested or issued under Article 41 of the Data Protection (Jersey) Law 2018.

The Minister's responsibilities

The Minister has legal responsibility for the national cyber security of the Island. Therefore, the Minister has a number of powers within the draft Law to help improve cyber security and raise cyber resilience and ensure the governance and delivery of JCSC demonstrates value for money for the Island.

The Ministerial powers and responsibilities can be summarised as follows:

In Part 2: Jersey Cyber Security Centre The Director of the JCSC is a Ministerial appointment and JCSC must be acknowledged by the Minister as the authority for cyber security in Jersey. The Minister is directly involved in the establishment of any TACs and can receive any advice the TAC shares with the Director. The Director is obliged to notify the Minister and relevant TAC, should the Director decide not to follow the advice of the TAC. Article 7 provides Ministerial power to give direction to the Director, if it is necessary in the interests of the security of Jersey and the requirements are proportionate to what the direction seeks to achieve.

The Minister must present the Director's annual report to the States Assembly and has the power by Order to amend the provisions of the annual report. The Minister must agree the strategic 3-year plan for JCSC to ensure it reflects Ministerial priorities, which will also be published.

The Minister must make an annual assessment of funding required by the Director, the JCSC and the TACs. Funding for JCSC is governed through the Department for the Economy, as per current arrangements, and any annual assessment will be considered as part of the annual financial review cycle of government funding, as led by Treasury.

In Part 3: Objectives and Functions of Director The Minister may by Order make additional or supplementary provisions in relation to the functions of the Director (Article 15). This is intended to ensure the functions of the Director remain relevant as the cyber threat landscape changes and evolves.

The Minister must be consulted by the Director before any cyber security standards are set or adopted and the Minister must consent to the provisions of any cyber security services provided by the Director to the States of Guernsey.

In Part 4: Operators of Essential Services An entity falling within the threshold for an OES must notify the Minister, with the Minister also having powers to designate an entity as an OES, if considered appropriate (as defined in Article 22 (5)). The Ministerial requirement to maintain a list of OESs will be delegated to the Director (under Article 26 (2)). The policy intent is to ensure the list of the Island's critical service providers is

managed securely and can be used to improve information sharing and raise the Island's cyber resilience.

In Part 5: Security Duties on Operators of Essential Services The Minister may direct an OES to take specified measures that are considered appropriate and proportionate for the purposes of identifying cyber threats; reducing the risk of cyber incidents; preparing for, preventing and minimising the impact of cyber incidents and ensuring the continuity of their essential service (Article 30). The Minister must consult relevant regulators, the Director and other appropriate bodies before making a direction.

In a similar fashion, the Minister may direct an OES to take specified measures in response to a cyber incident or the adverse effects of the incident (Article 32).

Both these provisions are to raise the cyber resilience of the essential services upon which the Island is reliant and to support the culture change needed to ensure cyber security risk management is elevated to Board level.

In Part 6: Enforcement The Minister may serve a financial penalty notice on an OES up to a current maximum of £10,000 if satisfied that the OES has contravened a provision of the draft Law. For contravention by a government service, the Minister cannot impose a financial penalty but may take enforcement steps considered necessary, on advice of the Director.

Governance

The Minister is responsible for the appointment of the Director and, in Schedule 1, has the ability to terminate the appointment under the stated conditions. The Jersey Appointments Commission must be consulted, as part of the appointment process.

The Director and employees of JCSC are all currently, and will remain, employees of the States and therefore must abide by civil service codes of practice. Therefore, all governance practices expected when in receipt of government funding to demonstrate value for money, and which relate to employees of the States of Jersey, will continue to apply to the Director and employees of the JCSC on enactment of the draft Law.

The Department for the Economy will remain responsible for the funding of the JCSC, and the Public Finances (Jersey) Law 2019 and supporting Public Finance Manual will continue to apply directly to the financial activities of the Director and JCSC. The Chief Officer of the Department will remain the Accountable Officer, as current, and Treasury will continue to hold the Director accountable for spend within their set delegated limits. The annual accounts for JCSC will be included within the annual accounts produced under the Public Finances (Jersey) Law 2019.

The Minister has a duty (Article 10) to make an annual financial assessment to ensure the Director has the necessary resources to discharge their functions under the draft Law effectively and efficiently and this assessment will be taken into consideration during the annual financial review process of government.

On enactment of the draft Law, the Director must produce a 3-year strategic plan, in consultation with the Minister which reflects Ministerial priorities and an annual report that details the activities and financial position of the JCSC in the last financial year (1 January – 31 December). Both are required to be published, with the annual report being presented each year by the Minister to the States Assembly.

Duties placed on Operators of Essential Services and Government Services

In order to raise the cyber resilience of the Island, OESs for Jersey are identified as those providing a critical service on which a cyber attack or cyber threat could or may result in a reputational, political, economic or well-being risk to Jersey.

Articles 29 to 32 of the draft Law detail the duties to be placed on identified OESs. These duties also apply to government services.

Duties include the requirement to take appropriate and proportionate cyber security measures to identify cyber threats; reduce the risk of cyber incidents; prepare for cyber incidents to minimise their impact and ensure continuity of service.

All OESs must report significant cyber incidents within 24 hours and respond to any Ministerial direction given under Article 30 or Article 32.

Commencement and implementation

Commencement of the Cyber Security (Jersey) Law 202- (the "draft Law") will be by Order from the Minister.

The following provisions are planned to come into force first: Interpretation (Part 1); provisions for the establishment of the Jersey Cyber Security Centre (Part 2); the objectives and functions of the Director and JCSC (Part 3) and the Information and closing provisions (Part 7).

The following provisions will be enacted three months later: designation of Operators of Essential Services (Part 4) and their respective security duties (Part 5) and subsequent enforcement provisions (Part 6).

This enactment is to enable the adoption of the supporting guidance by OESs and ensure they all are aware of their duties under the draft Law. Consultation with OESs will continue throughout the development of relevant guidance and as the date for enactment draws closer.

Consultation will continue after enactment to capture learnings and best practice.

Financial and staffing implications

The resourcing and funding for the Director and Jersey Cyber Security Centre is already budgeted for within the Government Plan and through the Department for the Economy. Funding provision is currently £1,028,000 annually to support the current operating structure of 7 FTEs during office hours Monday to Friday.

There are no additional financial or staffing implications for the Government of Jersey in relation to this proposition.

The Minister's duties and functions will be funded through the existing Department for the Economy's budget and resource.

Children's Rights Impact Assessment

A Children's Rights Impact Assessment (CRIA) has been prepared in relation to this proposition and is available to read on the States Assembly website.

Human Rights

The notes on the human rights aspects of the draft Law in the **Appendix** have been prepared by the Law Officers' Department and are included for the information of States Members. They are not, and should not be taken as, legal advice.

APPENDIX TO REPORT

Human Rights Notes on the Draft Cyber Security (Jersey) Amendment Law 202-

These Notes have been prepared in respect of the draft Cyber Security (Jersey) Law 202- (the "**draft Law**") by the Law Officers' Department. They summarise the principal human rights issues arising from the contents of the draft Law and explain why, in the Law Officers' opinion, the draft Law is compatible with the European Convention on Human Rights ("**ECHR**").

These notes are included for the information of States Members. They are not, and should not be taken as, legal advice.

Background

The draft Law, if adopted, provides that the Minister for Sustainable Economic Development ("the Minister") must appoint the Jersey Cyber Security Centre ("JCSC") as an authority for cyber security in Jersey (see Article 2 of the draft Law). The Minister must also appoint a Director of the JCSC (see Article 2 *supra*). Under Part 3 of the draft Law, the main functions of the JCSC are to act as (i) the single point of contact for Jersey in relation to cyber security and (ii) the computer security incident response team for Jersey. The objectives of the Director of the JCSC are to prepare for, protect from, defend against and facilitate recovery from cyber threats and attacks affecting Jersey. The Director's functions are advisory and include issuing guidance and setting or adopting standards in relation to cyber security. The Director must also prepare a strategic plan setting out how the Director proposes to carry out those functions (see Article 9 of the draft Law).

Part 4 of the draft Law provides for persons to be designated as operators of essential services ("OES") in relation to a sector or subsector. An essential service is defined as a service which is specified in Schedule 3, or is essential for the infrastructure, the maintenance of critical societal or economic activities, or the maintenance of the reputation of Jersey.

A person is deemed to be designated as an OES for a sector or subsector if (i) that person provides an essential service specified in Schedule 3, (ii) the service provided relies upon network and information systems and (iii) the person satisfies the threshold requirement specified in Schedule 3. Any person who is deemed to be designated as an OES must notify the Minister in writing of that fact. Even where a person does not satisfy the threshold specified in Schedule 3, the Minister may still designate them as an OES if, in the Minister's opinion, a cyber incident would have or is likely to have a significant disruptive effect on the provision of that service.

Part 5 of the draft Law sets out the security duties required of an OES. These duties include taking measures to (a) identify risks of cyber incidents, (b) reduce the risk of cyber incidents occurring, (c) prepare for cyber incidents and prevent and minimise their impact and d) ensure the continuity of their essential service.

Additionally, under Articles 30 and 32, the Minister may, by Order, specify particular measures that an OES must take both prior to and in response to a cyber incident.

Article 35, read with Article 41, gives the States a power to make regulations regarding the enforcement of security duties and making supplementary provisions.

Part 6 of the draft Law makes provision for the enforcement of the draft Law including a power to the Minister to impose civil financial penalties on OES who contravene provisions relating to security measures.

Part 7 of the draft Law makes provisions for information sharing.

Engagement with Article 6 and Article 1 of Protocol 1 to the European Convention

Part 5 of the draft Law has the potential to engage Article 1 of the First Protocol to the ECHR ("A1P1"), which provides for certain protections in relation to an individual's property and both the civil and criminal limbs of Article 6 which provides for the right to a fair trial/hearing.

Article 1 of Protocol 1 (A1P1): Protection of property

> "Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.
>
> The preceding provisions shall not, however, in any way impair the right of the State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure payment of taxes or other contributions or penalties."

The reference to every "natural or legal person" means that the of corporate bodies are protected and this is well established in the case law. As regards the entitlement to peaceful enjoyment of possessions (A1P1 first sentence) and the rule against deprivation of possessions (second sentence), in National Provincial Building Society v United Kingdom (1998) 25 EHRR 127 [78] the Court took the view that it is the first sentence that enunciates the general principle which then informs interpretation of the remainder of A1P1.

Whilst the first paragraph of A1P1 provides for the peaceful enjoyment of possessions the second paragraph of A1P1 states that this is subject to the ability of the State to: "enforce such laws as it deems necessary …in the general interest". As such, the right to peaceful enjoyment of possessions under A1P1 is not an absolute but a qualified right. A deprivation of possessions is only permitted if it is (i) lawful; (ii) in the public interest; (iii) in accordance with the general principles of international law; and (iv) reasonably proportionate ("fair balance" test).

A1P1 is likely to be engaged by the draft Law to the extent that its provisions interfere with individual property rights. An exercise of certain powers provided by the draft Law may result in 'deprivations', 'controls of use' or 'interferences with enjoyment' of the property of individuals. Those requirements in the draft Law that relate to security measures (Article 29, 30 and 32) may result in a control of use or interference with the property of an OES.

As stated above, A1P1 is a qualified right, and as such there may be limitations on the right to the extent that there is a legitimate aim, the limitation is prescribed in law and the measures used are proportionate. Taking first the question of whether there is a legitimate aim, A1P1 permits a control of use of property in accordance with the general interest. The "general interest" may be, and has been, interpreted widely, and individual States have a significant margin of appreciation[2] to determine the general interest.

The Court has previously held the general interest to include measures for environmental protection purposes, including planning controls for the preservation of areas of natural beauty (Herrick v United Kingdom, Application No. 11185/84) and a shore conservation programme (Uuhiniemi v Finland, Application No. 21343/9). The purposes of the limitations referred to above are to protect individuals, businesses and government from cyber threats and cyber incidents. Such controls and interferences with property rights can be justified on the basis that any control on use of an OES's property is necessary to ensure that information networks,

[2] The "margin of appreciation" is a legal doctrine, most notably used by the European Court of Human Rights which grants national authorities a degree of discretion in implementing human rights obligations. It acknowledges that national legal and cultural contexts vary and allows for flexibility, ensuring a minimum level of human rights protection while giving states latitude to balance individual rights with national interests. The doctrine is applied when a state's actions to promote the general interest potentially conflict with individual rights.

information systems and operational technology available to the public in Jersey are secure. Further, cyber incidents may also the threaten Jersey's reputation as a safe and secure place to conduct business.

The limitations and interferences are clearly prescribed in the draft Law and thereby satisfy the 'lawfulness' limb of the A1P1 test. They are also in line with other legal jurisdictions such as the EU, UK and USA in respect of cyber security.

The final point to consider is proportionality. In ECHR terms, the requirement for measures to achieve a 'fair balance' between the general interest and the interests of individuals is not synonymous with a 'least restrictive alternative' test. Restrictive measures must be justified on the basis of a compelling case in the public interest and as being "reasonably necessary but not obligatorily the least intrusive of Convention rights" (R. (Clays Land Housing Co-op) v The Housing Group (2005) [2005] 1WLR 2229). Under A1P1, the payment of compensation in appropriate cases will be relevant to the fairness of the balance achieved between the community interest and individuals' property rights. Where an interference with property amounts to a full deprivation of property, the Court has ruled that a 'fair balance' gives rise to a right to compensation in all but the most exceptional circumstances (Lithgow v United Kingdom 8 Eur. H.R. Rep. 329 (1986).

The limitations in the draft Law satisfy the proportionality requirement in that they are reasonable and proportionate to the objectives which they are designed to secure.

In conclusion Articles 29, 30 and 32 the draft Law are considered to be compatible with ECHR and the Human Rights (Jersey) Law 2000.

Article 6 (Right to a fair trial)

Article 6.1

> "In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."

Article 6 of ECHR thus secures the right to a fair and public hearing by an independent and impartial tribunal established by law in the determination of civil rights and any criminal charges.

Articles 22, 24 and 36 of the draft Law has the potential to engage the civil limb of Article 6. In respect of a decision to designate a person as an OES under Articles 22 or 24, there is a right of appeal to the Royal Court under Article 27.

In respect of a civil penalty may be imposed by the Minister under Article 36, the Minister must first (i) give full details of any decision to impose a penalty, (ii) consider any representations made by the OES and (iii) issue a confirmation of the decision together with details of the appeals process.

The maximum level of fine is £10,00 which is not considered disproportionate and falls within the parameters of similar provisions in other jurisdictions.

Article 37 of the draft Law gives an OES a right of appeal against a Ministerial decision to the Royal Court. Accordingly, it is considered that these provisions are compatible with the civil limb of Article 6 and with the Human Rights (Jersey) Law 2000.

The criminal limb of Article 6 is likely to be engaged by Article 39 of the draft Law. Article 39 states that a person commits an offence if they knowingly or recklessly provide false or misleading information to an entitled person in purported compliance with a requirement under the draft Law or where an entitled person (the Minister, the Director, the Jersey Cyber Security Centre or other persons entitled under the draft Law.) is exercising a function under the draft Law.

The penalty, on conviction, is a term of imprisonment for up to 5 years and an unlimited fine. The level of this penalty is considered proportionate and is consistent with similar provisions in Article 54 of the Telecommunications (Jersey) Law 2002 and Article 55 of the Competition (Jersey) Law 2005.

Offences under Article 39 of the draft Law will be subject to criminal prosecution in the normal way with proceedings brought before the Royal Court. Therefore, it is considered that Article 39 is compatible with Article 6 of ECHR.

EXPLANATORY NOTE

This Law, if adopted, would provide that the Minister must appoint the Jersey Cyber Security Centre (the "JCSC") as an authority for cyber security in Jersey, and appoint a Director of the JCSC (the "Director"). The objectives of the Director and the JCSC are to prepare for, protect from, defend against and facilitate recovery from, cyber threats or cyber attacks affecting Jersey.

Part 1 – Interpretation

Article 1 is the interpretation provision.

Part 2 – Jersey Cyber Security Centre

Article 2 provides that the Minister for Sustainable Economic Development (the "Minister") must appoint the JCSC as authority for cyber security in Jersey, and must appoint a Director. It provides that the Director and employees of the JCSC are States' employees and introduces *Schedule 1,* which makes further provision in respect of the office of Director.

Article 3 provides that the Director or any person performing a function of the Director must not be directed on how their functions are to be carried out, other than as set out in Article 5(4) (advice provided by TAC) or Article 7 (powers of Minister in relation to JCSC) .

Article 4 provides that the Minister or Director may establish Technical Advisory Councils ("TACs") that advise the Director on matters relating to the Director's functions or on cyber security matters affecting Jersey. It also introduces *Schedule 2*, which makes further provision in relation to TACs.

Article 5 provides that, when requested by the Director, a TAC must provide advice in accordance with its terms of reference. It further provides that if the advice is not followed, the Director must give reasons to the TAC and the Minister, provides a mechanism for the TAC to report its findings to the Minister if the Director does not follow its advice, gives a power to the Minister to order that the Director acts in accordance with the TAC's advice, and gives a power for the Director to use the advice to produce guidance for publication.

Article 6 provides that the Director must, following appropriate consultation, produce and publish codes of conduct for employees of the JCSC and for members of a TAC. It further provides that the employees and members must abide by the codes of conduct.

Article 7 sets out the Minister's powers in relation to the JCSC: that the Minister may review or commission a review of the performance of the Director, and that the Minister may give directions or guidance to the Director, providing that doing so is proportionate and necessary in the interests of the security of Jersey, or if the Minister has consulted appropriately.

Article 8 provides that the Director must produce accounts and an annual report, and sets out the required contents and requirement for publication and presentation to the Minister.

Article 9 provides that the Director must prepare a strategic plan, in respect of each 3-year period, setting out how the Director proposes to perform their functions. It also provides for revision of a strategic plan, and for agreement of the plan with the Minister. It further provides that a strategic plan must be published.

Article 10 provides that the Minister must, after consulting the Director, make an annual assessment of the funding required by the Director and the JCSC and submit that amount to the Council of Ministers under the Public Finances (Jersey) Law 2019.

Article 11 provides that the Director and JCSC must operate independent information technology systems that comply with the requirements set by the Forum of Incident Response and Security Teams (FIRST).

Part 3 – Objectives and functions

Article 12 sets out the objectives of the Director, which are to prepare for, protect from, defend against, and facilitate recovery from, cyber threats or cyber attacks affecting Jersey. It provides that a cyber threat or cyber attack "affects" Jersey if –

(a) it affects the States of Jersey, a public administration, a government service, a person having a place of business or address in Jersey, an operator of an essential service (see further *Part 4*), an individual present in Jersey, the .je internet domain, or a service using Autonomous System Names and Internet Protocol address prefix assigned to Jersey or for use in Jersey; or

(b) it results, or may result, in reputational, political, economic or well-being risks to Jersey.

Article 13 provides that the JCSC is the SPOC for Jersey. As such, the JCSC's functions include –

(a) consulting and co-operating with certain law enforcement authorities (which include the States of Jersey Police Force, the Honorary Police and the UK's National Crime Agency) and relevant regulatory bodies in Jersey;

(b) co-operating with the Ministers designated as competent authorities under Article 4 of the Emergency Powers and Planning (Jersey) Law 1990 and the Information Commissioner;

(c) liaising with the SPOCs and CSIRTs and national competent authorities of the UK and of Member States of the EU, and with bodies in other countries and territories that perform a substantially similar function to a SPOC or CSIRT.

Article 14 sets out that the JCSC is the CSIRT for Jersey. As such, its functions include –

(a) monitoring and scanning publicly accessible networks and information systems ("NIS") to identify malicious activity, vulnerabilities and configuration errors, and taking the action it considers necessary to resolve those vulnerabilities, configuration errors or cyber threats;

(b) taking reasonable steps to understand current global cyber threats; raising awareness in Jersey of cyber security risks and threats, and responses and mitigations;

(c) providing and co-ordinating the delivery of cyber security services;

(d) enabling, providing and co-ordinating the delivery of cyber security services;

(e) enabling and promoting the sharing of cyber security information in Jersey;

(f) increasing the level of cyber resilience in Jersey to reduce the risk and impact of cyber incidents; representing Jersey's cyber security interests in Jersey and internationally, including by participating in international co-operation networks including the CSIRTs network; and

(g) providing support to enable effective cyber security in Jersey.

Article 15 sets out that functions may be conferred on the Director by another enactment, that the Director may advise the Minister on matters relating to cyber security, and that this Article may be amended by Order to make additional provision in relation to the Director's functions.

Article 16 provides that the Director may discharge their functions by entering into an agreement with another person under which that other person discharges the function, if the Director is satisfied that it is appropriate to do so, and that the other person has the expertise and resources

necessary to discharge the function. The Director is not required to discharge a function under this Law if and to the extent that another person is required by an enactment to discharge a function that has the same or substantially the same effect.

Article 17 provides for the Director, having sought advice from TACs and specified others, to issue guidance in relation to cyber security and the exercise of its functions under Part 3.

Article 18 grants the Director a power to set or adopt standards in relation to cyber security, having sought advice from the Minister, the relevant TAC and specified others. Standards adopted or set must be published.

Article 19 provides for the Director and employees of the JCSC, on request, to assist in an investigation, that is necessary in relation to the Director's objectives and functions, being carried out by other persons, including the Information Commissioner, the Jersey Financial Services Commission, the States of Jersey Police Force and the Jersey Competition Regulatory Authority.

Article 20 provides that, in the specified circumstances, the Director may provide cyber security services to the States of Guernsey.

Article 21 enables the States, by Regulations, to amend Part 3 to make alternative or supplementary provision about the Commissioner's functions.

Part 4 – Operators of essential services

Article 22 provides for persons to be designated as operators of essential services ("OES") in relation to a sector or subsector. An essential service is defined in *Article 1* as a service that is specified in *Schedule 3*, or is essential for the infrastructure, the maintenance of critical societal or economic activities, or the maintenance of the reputation of Jersey. The sectors and subsectors are set out in *Schedule 3* and include, for example, the energy sector and its subsectors electricity, crude oil based fuel, and gas.

A person is taken to be designated as an OES for a sector or subsector if they provide an essential service in Jersey specified in *Schedule 3* corresponding to that sector or subsector, the provision of that service relies on NIS or operational technology, and the person satisfies the threshold requirement or condition specified in *Schedule 3* in relation to that sector or subsector. A person who is taken to be designated as an OES must notify the Minister in writing of that fact and provide certain details.

If a person provides an essential service specified in *Schedule 3* and the provision of that service relies on NIS or operational technology, but the person does not satisfy the threshold requirement or condition specified in *Schedule 3* in relation to the relevant sector or subsector, the Minister may designate them as an OES if, in the Minister's opinion, a cyber incident would have or is likely to have a significant disruptive effect on the provision of that service. This Article sets out the factors the Minister must take into account before designating a person as an OES.

Article 23 provides for the Minister to give a person an "information notice" so that the Minister can request information that enables them to determine whether a threshold requirement or condition in *Schedule 3* is met or whether the person may otherwise be designated by the Minister as an OES.

Article 24 provides that, in the specified circumstances, the Minister may designate a person as an OES even if the head office is outside Jersey.

Article 25 requires that, if an OES has a head office outside Jersey, they must notify the Minister in writing of a person in Jersey authorised by the OES to act on their behalf under this Law.

Article 26 requires the Minister to maintain a list of OES, and to review a person's designation as an OES on written request. It provides for the Minister to revoke designations and deemed designations of a person as an OES. The list may be administered day-to-day by the Director.

Article 27 provides a right of appeal to the Royal Court against decisions of the Minister to designate a person as an OES or not to revoke a person's designation as an OES.

Part 5 – Security duties on operators of essential services

Article 28 is an interpretation provision.

Article 29 requires an OES to take measures to identify risks to the security of the NIS or operational technology on which the provision of their essential service relies, reduce the risk of, and prepare for, cyber incidents affecting the security of the NIS or operational technology occurring, and ensure the continuity of their essential service. The Director must issue guidance on the operation of this Article.

Article 30 enables the Minister by direction (after appropriate consultation) to specify particular measures an OES must take for the purposes of *Article 29*.

Article 31 requires an OES to notify the Director of a cyber incident that has had or is likely to have a significant impact on the essential service that the OES provides. That notification must include information about the nature and impact of the cyber incident.

Article 32 enables the Minister to specify particular measures an OES must take in response to a cyber incident and its adverse effects in a direction.

Article 33 requires the Minister to have due regard to operational independence when making an Article 30 or Article 32 direction.

Article 34 requires the Director to publish guidance in relation to Part 4.

Article 35 enables the States, by Regulations, to make alternative or supplementary provision about the duties imposed on an OES under Part 4 and provision for the enforcement of the duties on an OES under Part 4, including by amending Part 4.

Part 6 – Enforcement

Article 36 provides that the Minister may serve an OES with a penalty notice imposing a financial penalty in the event of a contravention of the Law, and sets out the procedure for serving that penalty notice. The Minister may, by Order, amend the maximum amount of financial penalty.

Article 37 provides that an OES may appeal against a financial penalty to the Royal Court.

Article 38 provides that the Minister may take steps that they consider necessary against a government service that is in contravention of this Law.

Article 39 provides that knowingly or recklessly providing false or misleading information under this Law is an offence carrying a maximum penalty of 5 years' imprisonment and an unlimited fine. It further provides for liability for offences under this Law committed by bodies corporate and unincorporated associations and makes further provision about payment of fines, proceedings and rules of court for unincorporated associations. Paragraph (4) applies the provisions of this Article to an offence under Article 1 of the Criminal Offences (Jersey) Law 2009 of aiding, abetting, counselling or procuring the commission of an offence under this Law, or conspiring, attempting or inciting another to commit an offence under this Law.

Part 7 – Information sharing and closing provisions

Article 40 provides that, despite any restriction in contract or statute, a person may share information with the Director for the purpose of exercising the Director's functions under this Law. It further provides that the Director may share information with a law enforcement body, another country's SPOC or CSIRT and the persons the Director considers appropriate, if doing so is necessary for the Director to fulfil a function under the Law, in the interests of Jersey's

security or for purposes relating to prevention or detection of crime, the investigation of an offence or the conduct of a prosecution. Information shared by the Director must be relevant and proportionate to the purpose for which it is shared.

Article 41 enables the States to amend this Law, by Regulations, to make alternative or supplementary provision.

Article 42 is a transitional provision that provides that the Director and employees of the JCSC are treated as having been employed by the States in their positions from the date of their first employment with the JCSC.

Article 43 introduces *Schedule 4*, which contains consequential amendments. It also provides that the States may, by Regulations, amend enactments (other than this Law) to make consequential amendments.

Article 44 gives the name of this Law and provides for it to come into force on a day to be specified by the Minister by Order.

Jersey

DRAFT CYBER SECURITY (JERSEY) LAW 202-

Contents

Article

Jersey

DRAFT CYBER SECURITY (JERSEY) LAW 202-

A LAW to provide for the establishment and functions of the Jersey Cyber Security Centre, and for connected purposes.

Adopted by the States	*[date to be inserted]*
Sanctioned by Order of His Majesty in Council	*[date to be inserted]*
Registered by the Royal Court	*[date to be inserted]*
Coming into force	*[date to be inserted]*

THE STATES, subject to the sanction of His Most Excellent Majesty in Council, have adopted the following Law –

PART 1

INTERPRETATION

1 Interpretation

(1) In this Law –

"CSIRT" has the meaning given in Article 14(1);

"CSIRTs network" means the network established under Article 12(1) of the NIS Security Directive;

"cyber attack" means malicious or unauthorised activity that attempts to collect, disrupt, deny, degrade, destroy or reduce confidence in network and information systems or operational technology or the information held in or processed through those systems or technology;

"cyber incident" means an event that –

(a) arises from a cyber threat, whether accidental or malicious;

(b) involves unauthorised access or attempted unauthorised access to an organisation's network and information systems or operational technology, whether accidental or malicious;

(c) compromises the confidentiality, integrity, availability, authenticity or non-repudiation of –

(i) network and information systems or operational technology;

(ii) information held in or processed through those systems or that technology;

(iii) the users of those systems or that technology; or

(iv) another person; and

(d) has a negative impact on the cyber security of those systems, that technology, that information or that other person;

"cyber resilience" means the capacity of a person to –

(a) prepare for, protect against, detect, respond to or recover from a cyber threat in order to ensure the confidentiality, integrity, availability, authenticity or non-repudiation of network and information systems or operational technology and information held in or processed through those systems or that technology; and

(b) protect network and information systems or operational technology, the users of those systems or that technology, and other persons from loss, disruption or harm;

"cyber security" means the activity undertaken –

(a) to prepare for, protect against, detect, respond to or recover from a cyber threat in order to ensure the confidentiality, integrity, availability, authenticity or non-repudiation of network and information systems or operational technology and information held in or processed through those systems or that technology; and

(b) to protect network and information systems or operational technology, the users of those systems or that technology, and other persons from loss, disruption or harm;

"cyber threat" means an actual or potential circumstance or event –

(a) involving compromise of the confidentiality, integrity, availability, authenticity or non-repudiation of –

(i) network and information systems or operational technology;

(ii) information held in or processed through those systems or that technology;

(iii) the users of those systems or that technology; or

(iv) another person; and

(b) having the potential to have a negative impact on the cyber security of those systems, that technology, that information or that other person;

"Director" means the person appointed by the Minister as director of the JCSC under Article 2;

"electronic communications network" means –

(a) a transmission system to convey, by the use of electrical, magnetic or electro-magnetic energy, signals of any description;

(b) any of the following that are used, by the person providing the system and in association with it, to convey the signals –

(i) apparatus comprised in the system;

(ii) apparatus used for the switching or routing of the signals;

(iii) software and stored data;

(iv) other resources, including network elements that are not active;

"electronic communications service" means a service of 1 or more of the following types provided by means of an electronic communications network, except so far as it is a content service –

(a) an internet access service;

(b) a number-based interpersonal communications service; and

(c) another service consisting of, or having as its principal feature, the conveyance of signals, such as a transmission service used for machine-to-machine services;

"essential service" means –

(a) the services specified in Schedule 3; or

(b) a service that is essential for –

(i) the infrastructure of Jersey;

(ii) the maintenance of critical societal or economic activities in Jersey; or

(iii) the maintenance of the reputation of Jersey;

"financial year" means the period beginning with the day on which this Law comes into force and ending with 31 December of that year, and each subsequent period of 12 months ending with 31 December;

"government service" means –

(a) a Minister; or

(b) an organisational entity that discharges the functions of a Minister;

"Information Commissioner" means the person appointed under Article 5 of the Data Protection Authority (Jersey) Law 2018;

"JCRA" means the Jersey Competition Regulatory Authority established under Article 2 of the Competition Regulatory Authority (Jersey) Law 2001;

"JCSC" means the Jersey Cyber Security Centre appointed under Article 2;

"JFSC" means the Jersey Financial Services Commission established under Article 2 of the Financial Services Commission (Jersey) Law 1998;

"Minister" means the Minister for Sustainable Economic Development;

"network and information system" means –

(a) an electronic communications network;

(b) a device or group of interconnected or related devices, of which at least 1 performs automatic processing of digital data under a program; or

(c) digital data stored, processed, retrieved or transmitted by the network or device for the purposes of the operation, use, protection and maintenance of the network or device;

"NIS Security Directive" means Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (OJ L 333, 27.12.2022, p.80);

"OES" means an operator of essential services, as defined in Article 22(1);

"operational technology" means technology that interfaces with the physical world and includes –

(a) industrial control systems;

(b) supervisory control and data acquisition; and

(c) distributed control systems;

"public administration" means –

(a) a person or body listed in paragraph 20 or 21 of Schedule 3; or

(b) a government service;

"Public Finances Law" means the Public Finances (Jersey) Law 2019;

"publish" means publish in the manner that the Minister considers likely to bring it to the attention of the persons affected;

"SPOC" means a single point of contact for cyber security;

"States of Jersey Police Force" means the police force continued in being by Article 2 of the States of Jersey Police Force Law 2012;

"TAC" means a Technical Advisory Council established under Article 4.

(2) The Minister may by Order amend this Article to make alternative or supplementary provision in relation to the definitions of expressions used in this Law.

PART 2

JERSEY CYBER SECURITY CENTRE

2 Administration of cyber security

(1) The Minister must appoint the JCSC as an authority for cyber security in Jersey.

(2) The Minister must appoint the Director.

(3) The Director and the employees of the JCSC are States' employees within the meaning of Article 2 of the Employment of States of Jersey Employees (Jersey) Law 2005, and a States' employee provided to the JCSC under Article 10 of this Law who performs a function under the Director's direction is treated as an employee of the JCSC.

(4) The Director may delegate a function under this Law to the JCSC, but the delegation does not –

(a) affect the responsibility of the Director for the discharge of the function; or

(b) prevent the discharge of the function by the Director personally.

(5) The Director or the Minister must delegate the Director's functions under this Law to a specified employee of the JCSC if the Director –

(a) is absent from Jersey; or

(b) is otherwise unable to discharge their functions.

(6) Schedule 1 makes further provision in respect of the Director.

(7) The States may amend Schedule 1 by Regulations made under Article 41.

3 Operational independence of Director

Other than under Article 5(4) or 7, the Director, or a person discharging or performing a function of the Director, must not be directed on how a function of the Director or the JCSC is to be carried out.

4 Technical Advisory Councils (TACs)

(1) The Minister or the Director may establish TACs to advise the Director on matters that relate to –

(a) the Director's responsibilities or functions under this Law;

(b) cyber security in Jersey; or

(c) cyber security matters outside Jersey that may affect Jersey.

(2) The Director must obtain the Minister's approval in writing before establishing a TAC.

(3) The terms of reference for each TAC must –

(a) contain the specific areas of cyber security for which that TAC is responsible; and

(b) be published on the JCSC website no later than 3 months after the TAC is established.

(4) But the terms of reference for a TAC must not be published if, in the opinion of the Director, their publication would jeopardise national security.

(5) Schedule 2 makes further provision in relation to TACs.

5 Advice provided by TAC

(1) A TAC must provide advice when requested by the Director to do so.

(2) The advice must be provided to the Minister and the Director in accordance with the terms of reference for that TAC.

(3) If the Director decides not to follow the advice –

(a) the Director must give reasons, in writing, to the Minister and the TAC; and

(b) the TAC may provide the advice and the Director's reasons to the Minister if the TAC considers that the Director's decision is –

(i) erroneous; and

(ii) not in the interests of Jersey.

(4) After considering the TAC's advice and the Director's reasons not to follow that advice, the Minister may order the Director to act in accordance with the advice.

(5) If the Director considers that publication of the advice is in the public interest, the Director may use the advice to produce guidance under Article 17 or 34.

6 Codes of conduct

(1) The Director must, no later than 3 months after the Director's appointment, produce and publish on the JCSC website –

(a) a code of conduct for employees of the JCSC (the "JCSC code of conduct"); and

(b) a code of conduct for members of a TAC (the "TAC code of conduct").

(2) The Director and employees of the JCSC must abide by the JCSC code of conduct.

(3) In the event that the JCSC code of conduct is inconsistent with a code of practice issued under Article 8 of the Employment of States of Jersey Employees (Jersey) Law 2005 (a "States code of practice"), the States code of practice takes precedence.

(4) A member of a TAC must abide by the TAC code of conduct and act in accordance with the terms of reference for that TAC.

(5) Before producing the JCSC code of conduct, the Director must consult the Minister and the employees of the JCSC.

(6) Before producing the TAC code of conduct, the Director must consult the Minister and the members of the TACs.

(7) When consulting on a code of conduct under paragraph (5) or (6), the Director must allow 28 days, starting on the day of the consultation, for responses.

7 Powers of Minister in relation to JCSC

(1) The Minister may review, or commission another person to review, the performance of the Director's functions in relation to the Director's objectives under Article 12(1).

(2) The Minister may give a direction to the Director if the Minister considers that –

(a) the direction is necessary in the interests of the security of Jersey; and

(b) the requirements imposed by the direction are proportionate to what the direction seeks to achieve.

(3) If the conditions in paragraph (2) are not met, the Minister may give directions or guidance to the Director only if the Minister has consulted with the Director and the other persons that the Minister considers appropriate.

(4) The Director must comply with a direction given under paragraph (2) or (3).

8 Accounts and annual report

(1) The Director must ensure that –

(a) proper accounts and proper records in relation to the accounts are kept;

(b) accounts are prepared in respect of each financial year ("annual accounts"); and

(c) the annual accounts are prepared using the accounting standards by which the accounts of the States are prepared (as set out in the Public Finances Manual issued under Article 31 of the Public Finances Law).

(2) The Director must produce a report on the exercise and performance of the functions of the Director and the JCSC in relation to each financial year (an "annual report").

(3) The annual report must include –

(a) the annual accounts;

(b) a report on the activities of the Director in the preceding year;

(c) a report setting out, in anonymised format, all mandatory cyber incidents reported to the Director under Article 31;

(d) a report from each TAC setting out the advice and reports given to the Director during the preceding year; and

(e) other statements or reports relevant to the exercise of the functions of the Director that the Director considers appropriate.

(4) But the annual report must not include –

(a) confidential information;

(b) information that may prejudice –

(i) the security of those providing information;

(ii) the commercial interests of those providing information;

(iii) the prevention of crime; or

(iv) national security; or

(c) information that directly or indirectly identifies an individual.

(5) The Director must present the annual report to the Minister no later than 6 months after the end of the financial year to which it relates.

(6) The Minister must present a copy of the annual report to the States Assembly as soon as reasonably practicable after receiving it.

(7) The Director must publish each annual report as soon as reasonably practicable after it has been presented to the Minister.

(8) The Minister may by Order amend this Article to make further or alternative provision with regard to the annual report.

9 Strategic plan

(1) The Director must, in respect of a 3-year period, prepare a plan (a "strategic plan") setting out how the Director proposes to perform their functions during the 3-year period.

(2) A strategic plan must –

(a) be developed after consultation with the Minister;

(b) reflect Ministerial priorities; and

(c) be presented to the Minister –

(i) in the case of the first Director appointed under this Law, no later than 6 months after this Law comes into force; or

(ii) no later than 3 months before the commencement of the 3-year period to which the plan relates.

(3) The Director may, at any time during a 3-year period, review the strategic plan and present to the Minister a revised strategic plan.

(4) Within 3 months of a Director's appointment, that Director may present to the Minister a new strategic plan but that plan will only have effect until the expiry of the strategic plan that it replaces.

(5) A strategic plan prepared under this Article must be agreed with the Minister and, no more than 2 months later, published in that agreed form.

(6) In this Article, "3-year period" means –

(a) in relation to the first strategic plan prepared under this Article, the period starting with the date the plan is prepared and ending at the end of 31 December in the year that is 3 years after the date the plan is prepared; and

(b) in relation to subsequent strategic plans, the period starting with 1 January of the first year of the plan and ending at the end of 31 December of the third year of the plan.

10 Annual assessment of funding by Minister

(1) The Minister must make an annual assessment of the funding required by the Director, the JCSC and the TACs.

(2) In making an annual assessment, the Minister must consider the funding required to ensure that the Director has the financial and administrative resources, and other support including staff, services, equipment and accommodation, necessary to enable the Director, the JCSC and the TACs to discharge their functions under this Law effectively and efficiently.

(3) Before the Minister submits an amount in respect of the Director, the JCSC and the TACs to the Council of Ministers under Article 10(1)(d) of the Public Finances Law, the Minister must consult the Director.

(4) The States may amend this Article by Regulations made under Article 41.

11 Independence of JCSC IT systems

The Director and the JCSC must operate independent information technology systems that comply with the requirements set by the Forum of Incident Response and Security Teams Inc (incorporated on 7 August 1995 as a non-profit organisation under section 501(c)(3) of Title 26 of the United States Code).

PART 3

OBJECTIVES AND FUNCTIONS

12 Objectives of Director

(1) The objectives of the Director are to prepare for, protect from, defend against, and facilitate recovery from, cyber threats or cyber attacks affecting Jersey.

(2) The Director must so far as reasonably practicable administer the operation of this Law and exercise their functions in a way that –

(a) is compatible with the Director's objectives; and

(b) the Director considers most appropriate to further the objectives.

(3) For the purposes of paragraph (1), a cyber threat or a cyber attack affects Jersey if –

(a) it affects –

(i) the States of Jersey;

(ii) a public administration;

(iii) a relevant person;

(iv) an operator of an essential service not otherwise falling within this sub-paragraph;

(v) an individual not otherwise falling within this sub-paragraph who is present in Jersey, regardless of whether the individual is ordinarily resident in Jersey;

(vi) an Autonomous System Name and associated Internet Protocol address prefix assigned to Jersey by the Réseaux IP Européens Network Coordination Centre;

(viii) the .je country code top-level domain as assigned by the Internet Assigned Numbers Authority; or

(b) it results, or may result, in reputational, political, economic or well-being risk to Jersey.

(4) In this Article –

"external entity" means a person that –

(a) is not an individual;

(b) has a place of business or an address outside Jersey; and

(c) having regard to the extent to which their business is carried on, in and outside Jersey, the Minister considers a cyber attack in respect of the person would not be material to Jersey;

"relevant person" means a person, other than an external entity, having a place of business or address in Jersey.

(5) The Minister may by Order amend paragraphs (3) and (4).

13 Functions of JCSC: SPOC

(1) The JCSC is the SPOC for Jersey.

(2) As the SPOC for Jersey, the JCSC –

(a) must consult and co-operate, as the JCSC considers appropriate, with –

(i) relevant law enforcement authorities; and

(ii) relevant regulatory bodies in Jersey;

(b) must co-operate with a designated competent authority to enable them to fulfil their obligations under this Law;

(c) may, if the JCSC considers it appropriate to do so, liaise with –

(i) the relevant authorities in the United Kingdom, a Member State of the European Union, and other countries or territories;

(ii) the group established under Article 14(1) of the NIS Security Directive;

(iii) the Emergency Planning Officer appointed under Article 3 of the Emergency Powers and Planning (Jersey) Law 1990; and

(iv) the CSIRTs network.

(3) Nothing in this Article affects a duty on a person to make a report under another enactment.

(4) In paragraph (2)(b), "designated competent authority" means –

(a) a Minister designated as a competent authority under Article 4 of the Emergency Powers and Planning (Jersey) Law 1990; or

(b) the Information Commissioner.

(5) In paragraph (2)(c), "relevant authority" –

(a) in relation to the United Kingdom and a Member State of the European Union, means its SPOC, CSIRT and national competent authority;

(b) in relation to other countries or territories, means its SPOC, CSIRT and national competent authority, or another body that appears to the JCSC to perform a substantially similar function.

14 Functions of JCSC: CSIRT

(1) The JCSC is the computer security incident response team (the "CSIRT") for Jersey, and as CSIRT for Jersey has the functions in paragraphs (2) to (6).

(2) The JCSC must, as far as reasonably practicable –

(a) monitor and scan publicly accessible network and information systems to identify malicious activity, vulnerabilities and configuration errors; and

(b) take the action it considers necessary to resolve the vulnerabilities, configuration errors or cyber threats arising from them.

(3) The JCSC must take reasonable steps to understand current global cyber threats and how these may affect Jersey, and take the action it considers necessary in response to those threats.

(4) The JCSC must take reasonable steps to –

(a) raise awareness in Jersey of cyber threats, the risks arising from them, responses to them and mitigations against them;

(b) enable and promote the sharing of cyber security information in Jersey;

(c) support and co-ordinate the delivery of cyber security services in Jersey;

(d) increase the level of cyber resilience in Jersey to reduce the risk and impact of cyber incidents.

(5) The JCSC must represent Jersey's cyber security interests in Jersey and internationally, including by participating in international co-operation networks including the CSIRTs network.

(6) The JCSC may advise persons affected or potentially affected by a cyber attack or cyber threat.

(7) In undertaking its function under paragraph (2), the JCSC may –

(a) analyse information received by it relating to cyber incidents affecting Jersey;

(b) take the action it considers necessary to mitigate, or assist in the mitigation of, the effect of those cyber incidents; and

(c) advise a person affected or potentially affected by a cyber incident.

15 Functions of Director: general

(1) The Director has the functions conferred on the Director under this Law or transferred to the Director under another enactment.

(2) The Director may advise the Minister on matters relating to cyber security, whether on request or otherwise.

(3) The Minister may by Order amend this Article to make additional or supplementary provision in relation to the functions of the Director.

16 Discharge of Director's functions by another person

(1) The Director may fully or partly discharge a function by entering into an agreement with another person, on terms that the Director thinks fit, under which that other person fully or partly discharges the function.

(2) But the Director may not enter into an agreement under paragraph (1) unless the Director is satisfied that –

(a) it is appropriate to do so; and

(b) the other person has the expertise and resources necessary to discharge the function.

(3) If the Director enters into an agreement under paragraph (1) –

(a) that does not affect the responsibility of the Director for the discharge of the function; or

(b) prevent the discharge of the function by the Director personally.

(4) The Director is not required to discharge a function under this Law if another person is required by an enactment to discharge a function that has the same or substantially the same effect.

17 Duty to issue guidance in relation to cyber security

(1) The Director must issue guidance in relation to cyber security, including in relation to the exercise of their functions under this Part, and may revise and re-issue that guidance.

(2) Before issuing or re-issuing guidance under paragraph (1), the Director must, if the Director considers appropriate –

(a) seek advice from a relevant TAC; or

(b) consult –

(i) the regulators;

(ii) any sectoral or subsectoral OES; or

(iii) other persons.

18 Power to set or adopt cyber security standards

(1) The Director may set or adopt standards in relation to cyber security ("cyber security standards").

(2) The Director must from time to time review cyber security standards set or adopted under paragraph (1).

(3) Before setting or adopting cyber security standards the Director –

(a) must seek advice from a relevant TAC;

(b) must consult –

(i) the Minister; and

(ii) the regulators and any sectoral or subsectoral OES that the Director considers appropriate; and

(c) may consult the other persons that the Director considers appropriate.

(4) The Director must publish cyber security standards set or adopted under this Article.

(5) When publishing cyber security standards, the Director must –

(a) specify the persons, or classes of person, to whom the Director considers the cyber security standards apply; and

(b) provide guidance in relation to the cyber security standards set or adopted.

19 Power to assist in investigations

(1) The Director and employees of the JCSC may assist in an investigation into or relating to cyber security being carried out by a person listed in paragraph (2) if –

(a) the person requests the JCSC's assistance; and

(b) the Director is satisfied that the assistance is necessary to fulfil the Director's objectives and functions.

(2) The persons are –

(a) the Information Commissioner;

(b) the JFSC;

(c) the States of Jersey Police Force;

(d) the JCRA;

(e) other persons that the Director considers appropriate.

20 Power to provide cyber security services to States of Guernsey

(1) The Director may provide cyber security services, analogous to the Director's functions under this Law, to the States of Guernsey if –

(a) the Director considers it appropriate to do so; and

(b) the Minister consents to the provision of the services.

(2) The Director may provide the services on whatever terms, including as to payment, as the Director thinks fit.

(3) But the Director must not provide services under this Article if doing so would, in the Director's opinion, have a negative impact on the Director's ability to perform their functions under this Law.

21 Power to amend this Part by Regulations

The States may, by Regulations made under Article 41, amend provisions of this Part (other than this Article) to make alternative or supplementary provision about the functions of the Director that the States considers appropriate.

PART 4

OPERATORS OF ESSENTIAL SERVICES

22 Designation of OES

(1) A person is an operator of an essential service (an "OES") for a sector or subsector specified in Schedule 3 if –

(a) they are –

(i) taken to be designated as an OES under paragraph (2) for that sector or subsector; or

(ii) designated as an OES under paragraph (5) for that sector or subsector; and

(b) that designation has not been revoked under Article 26 or 27.

(2) A person is taken to be designated as an OES for a sector or subsector if –

(a) they provide a service in Jersey of a kind specified in Schedule 3 corresponding to that sector or subsector;

(b) the person resides or has a head office in Jersey;

(c) the provision of that service relies on network and information systems or operational technology; and

(d) the person meets the threshold requirements or conditions specified in Schedule 3 in relation to that sector or subsector.

(3) A person who falls within paragraph (2) must give the Minister written notice of that fact and their name, address and contact details (including email address and telephone number).

(4) A notification required under paragraph (3) must be given –

(a) in the case of a person who falls within paragraph (2) on the date on which this Article comes into force, before the end of 28 days beginning with that date;

(b) in other cases, before the end of 28 days beginning with the date on which the person first falls within paragraph (2).

(5) The Minister may designate a person as an OES if the person is not taken to be designated under paragraph (2) but –

(a) they provide a service in Jersey of a kind specified in Schedule 3 corresponding to that sector or subsector;

(b) the person resides or has a head office in Jersey;

(c) the provision of that service relies on network and information systems or operational technology; and

(d) in the opinion of the Minister, a cyber incident would have or is likely to have a significant disruptive effect on the provision of that service.

(6) In reaching their opinion in paragraph (5)(d), the Minister must have regard to the following factors –

(a) the number of users relying on the service;

(b) the degree of reliance of other relevant sectors or subsectors in Schedule 3 on the service;

(c) the likely impact, in terms of degree and duration, on economic and societal activities or public safety;

(d) the market share of the service;

(e) the geographical area that may be affected if a cyber incident affects the service;

(f) the importance of the provision of the service for maintaining a sufficient level of that service, taking into account the availability of alternative means of provision of that service;

(g) the likely consequences for the security of Jersey if a cyber incident affects the service; and

(h) other factors that the Minister considers appropriate.

(7) The Minister may in relation to a person to whom paragraph (5) applies –

(a) give the person written notice that the Minister proposes to designate them as an OES, with reasons; and

(b) give them 28 days to submit written representations about the proposed designation.

(8) The Minister must –

(a) have regard to representations received under paragraph (7)(b); and

(b) decide if the person is to be designated as an OES.

(9) The Minister must give the person written notice of their decision, with reasons, no later than 28 days after making the decision.

23 Information notices

(1) The Minister may by notice in writing served on a person (an "information notice") require the person to provide the Minister with the information the Minister reasonably requires to assist the Minister in determining whether –

(a) the person meets a threshold requirement specified in Schedule 3; or

(b) the person falls within Article 22(5) or 24.

(2) An information notice must –

(a) describe the information that is required by the Minister;

(b) give the Minister's reasons for requesting the information; and

(c) specify the time within which, and the form and manner in which, the requested information must be provided.

(3) A person who, without reasonable cause, does not comply with the requirements of an information notice is liable to a penalty under Article 36.

(4) The Minister may withdraw an information notice by giving written notice to the person on whom the information notice was served.

24 Person outside Jersey may be designated as OES

(1) This Article applies if –

(a) the Minister wishes to designate a person as an OES; but

(b) the person has its head office outside Jersey.

(2) Despite Article 22(5)(b), the Minister may designate the person as an OES if –

(a) it provides an essential service for the energy sector (see Schedule 3, Part 1) or the digital sector (see Schedule 3, Part 6); or

(b) it provides an essential service for another sector specified in Schedule 3, and has been notified in writing by the Minister that this Article applies to them.

25 OES: authorised person to act in Jersey

(1) An OES designated under Article 24 must give written notice to the Minister of a person in Jersey authorised by the OES to act on their behalf under this Law (the "authorised person").

(2) Written notice under paragraph (1) –

(a) must include –

(i) the name of the OES; and

(ii) the name, address and contact details (including email address and telephone number) of the authorised person; and

(b) must be given no later than the end of the period of 28 days beginning with the date on which the OES became an OES, whether under Article 22(2) or Article 24.

(3) The OES must notify the Minister in writing of changes to the information notified under paragraph (2)(a) as soon as practicable and in any event no later than the end of 28 days beginning with the date of the change.

(4) The Minister or the Director may contact the authorised person instead of or in addition to the OES for the purposes of carrying out the Minister's or the Director's responsibilities under this Law.

(5) An authorisation under paragraph (1) does not affect any legal action that could be initiated against the OES.

26 Review and revocation of OES designation

(1) The Minister must maintain a list of OESs.

(2) The Minister may delegate the day-to-day maintenance of the list to the Director.

(3) If a person has reasonable grounds to believe that their designation as an OES is no longer justified under Article 22 or 24, they must notify the Minister in writing as soon as practicable providing evidence supporting that belief.

(4) If the Minister receives a notification under paragraph (3), the Minister must review the person's designation as an OES within 3 months after the date of receipt.

(5) The Minister may revoke the designation of a person under Article 22(2), by notice in writing, if the Minister decides that a cyber incident affecting the provision of the relevant essential service by that person would not have or is not likely to have significant disruptive effects on the provision of the essential service.

(6) The Minister may revoke the designation of a person under Article 22(5) or 24, by notice in writing, if the conditions mentioned in that Article are no longer met by that person.

(7) Before revoking a person's designation under paragraph (5) or (6) the Minister must –

(a) notify the person in writing of the proposed revocation, with reasons;

(b) invite the person to submit representations in writing about the proposed revocation, within the time specified by the Minister; and

(c) consider representations submitted under sub-paragraph (b).

(8) In order to make the decision mentioned in paragraph (5), the Minister must have regard to the factors mentioned in Article 22(6).

27 Right of appeal in relation to designation as OES

(1) An OES may appeal to the Royal Court against a decision of the Minister –

(a) under Article 22(5) or Article 24 to designate them as an OES;

(b) under Article 26 not to revoke their designation as an OES.

(2) An appeal under this Article must be made by sending the Royal Court a notice of appeal –

(a) in accordance with rules of court; and

(b) no later than 28 days after the day on which the decision is made.

(3) A notice of appeal must set out –

(a) the provision of this Law under which the decision appealed against was taken; and

(b) the grounds of appeal, which must be set out in sufficient detail to indicate –

(i) to what extent the appellant contends that the decision appealed against was based on an error of fact or was wrong in law, or both; and

(ii) to what extent the appellant is appealing against the exercise of a discretion by the Minister.

(4) The Royal Court must decide an appeal under this Article by reference to the grounds of appeal set out in the notice of appeal.

(5) In determining an appeal under this Article, the Royal Court must apply the principles applicable on an application for judicial review.

(6) When it determines an appeal under this Article, the Royal Court may –

(a) confirm the decision appealed against;

(b) quash the decision appealed against in whole or in part;

(c) if it quashes the whole or part of the decision –

(i) remit the matter back to the Minister with a direction to reconsider and make a new decision in accordance with the ruling of the Royal Court; or

(ii) substitute for the decision any decision that the Minister could have made.

(7) The Royal Court may make the orders it thinks appropriate, including ancillary orders and orders as to costs.

(8) An appeal under this Article does not suspend the effect of the decision to which the appeal relates, unless the Court orders otherwise.

(9) The Minister must comply with a direction under paragraph (6)(c)(i).

(10) The power of the Royal Court to make rules of court under Article 13 of the Royal Court (Jersey) Law 1948 includes power to make rules dealing generally with all matters of procedure and incidental matters arising in relation to appeals under this Article.

PART 5

SECURITY DUTIES ON OPERATORS OF ESSENTIAL SERVICES

28 Interpretation of Articles 29 to 32

For the purposes of the duties contained in Articles 29 to 32, "OES" is to be read as including a government service.

29 Duty to take security measures

(1) An OES must implement measures that are appropriate and proportionate for the purposes of –

(a) identifying cyber threats to the security of the network and information systems or operational technology on which the provision of their essential service relies;

(b) reducing the risk of cyber incidents occurring that affect the security of those network and information systems or operational technology;

(c) preparing for cyber incidents, and preventing and minimising their impact; and

(d) ensuring the continuity of their essential service.

(2) The measures implemented under paragraph (1) must ensure a level of security of network and information systems and operational technology appropriate to the cyber threat and risk posed by that threat.

(3) The Director must issue guidance on the operation of this Article, including how to assess the appropriate level of security.

(4) In this Article, "security of network and information systems and operational technology" means the ability of network and information systems or operational technology to resist, at a given level of confidence, an event that may compromise the confidentiality, integrity, availability, authenticity, or non-repudiation of –

(a) information held in or processed though or those network and information systems or operational technology; or

(b) services offered by, or accessible through, those network and information systems or operational technology.

30 Duty to take specified security measures

(1) The Minister may direct an OES to take specified measures, or measures of a specified description, that the Minister considers are appropriate and proportionate for a purpose listed in Article 29(1).

(2) In this Article, "specified" means specified in a direction under paragraph (1).

(3) Before making a direction under paragraph (1), the Minister –

(a) must consult the Director and the regulators that the Minister considers appropriate; and

(b) may consult other persons that the Minister considers appropriate.

(4) Nothing in this Article or a direction under paragraph (1) affects the duty imposed under Article 29.

31 Duty to notify Director of cyber incidents

(1) An OES must notify the Director of a cyber incident that the OES considers has had, or is likely to have, a significant impact on the cyber resilience of the OES or on the essential service that the OES provides.

(2) In determining for the purposes of paragraph (1) whether a cyber incident has a significant impact on an essential service, the OES must have regard (insofar as it is within the OES's knowledge) to the following matters in particular –

(a) the number of users affected by the disruption of the essential service;

(b) the duration of the cyber incident; and

(c) the geographical area affected by the cyber incident.

(3) A notification under paragraph (1) must include all of the following that is within the knowledge of the OES at the time notification is given –

(a) the operator's name and the essential service it provides;

(b) the time and date the cyber incident occurred;

(c) the current status of the cyber incident;

(d) the duration of the cyber incident;

(e) the threat actor, if known;

(f) information about the nature and impact of the cyber incident;

(g) information about the impact, or likely impact, of the cyber incident outside Jersey; and

(h) other information that the OES considers may be helpful to the Director.

(4) The OES must give the notification required under paragraph (1) as soon as reasonably practicable and no later than 24 hours after the OES becomes aware of the occurrence of a cyber incident that has had or is likely to have a significant impact on the continuity of the essential service.

(5) The Minister may by Order amend paragraph (4) to vary the time within which a notification must be given.

(6) The States may, by Regulations made under Article 41, amend this Article to make further or alternative provision about the notification of cyber incidents.

(7) In this Article, "threat actor" means a person or group of persons who take actions intended to cause harm to network and information systems or operational technology.

32 Duty to take specified security measures in response to cyber incidents

(1) The Minister, having consulted the Director, may direct an OES to take specified measures in response to –

(a) a significant cyber incident or a description of a significant cyber incident that occurs in relation to a network and information system or operational technology on which the provision of an essential service, by the OES, relies;

(b) adverse effects of that cyber incident on that network and information system or operational technology.

(2) A direction under paragraph (1) must –

(a) specify the adverse effects; and

(b) specify the measures, or the description of measures, to be taken –

(i) in response to a cyber incident, for the purpose of preventing the adverse effects on the provision of the essential service arising from that cyber incident;

(ii) in response to an adverse effect, for the purpose of remedying or mitigating that adverse effect.

(3) But a measure, or description of a measure, may only be specified under paragraph (2)(b) if the Minister considers that taking that measure or a measure of

that description would be appropriate and proportionate for the purpose for which it is to be taken.

33 Directions under this Part

If the Minister directs an OES under Article 30 or 32, the Minister must have due regard to any applicable statutory operational independence.

34 Guidance in relation to this Part

(1) The Director must publish guidance about the measures to be taken by an OES under this Part.

(2) The Director may revise and re-publish guidance published under this Article.

(3) Before publishing or re-publishing guidance, the Director may –

(a) seek advice from a TAC; or

(b) consult –

(i) the regulators that the Director considers appropriate;

(ii) any sectoral or subsectoral OES that the Director considers appropriate; or

(iii) the other persons that the Director considers appropriate.

35 Power to amend this Part by Regulations

(1) The States may, by Regulations made under Article 41 –

(a) make alternative or supplementary provision about the duties imposed on an OES under this Part; or

(b) make provision for the enforcement of the duties imposed on an OES under this Part.

(2) Regulations may make the provision referred to in paragraph (1) by amending this Part.

PART 6

ENFORCEMENT

36 Power of Minister to impose civil financial penalties on OES

(1) If the Minister is satisfied that an OES has contravened a provision of this Law, the Minister may serve a penalty notice on the OES.

(2) A penalty notice must specify in writing –

(a) the reasons for imposing a penalty;

(b) the amount of the penalty;

(c) the date of the notice;

(d) the date by which the penalty amount must be paid;

(e) that the payment of the penalty under the notice does not affect the requirements of any existing direction under Article 30 or 32;

(f) how and when the OES may make representations about the content of the notice.

(3) The Minister must consider any representations made under paragraph (2)(f) and –

(a) if the Minister considers it appropriate in the light of the representations, issue a written notice of withdrawal of the penalty notice to the OES; or

(b) if the Minister considers that a penalty is still justified, issue a written confirmation notice to the OES.

(4) A confirmation notice must –

(a) include reasons for the Minister's final penalty decision;

(b) require the OES to pay –

(i) the amount specified in the penalty notice; or

(ii) the amount that the Minister considers appropriate in the light of the representations made under paragraph (2)(f);

(c) specify the period within which the penalty amount must be paid;

(d) provide details of the appeal process under Article 37; and

(e) specify the consequences of failing to make the payment within the period specified.

(5) The Minister may impose a penalty under paragraph (1) on a person who performs or performed a senior management function in relation to an OES if the Minister is satisfied that the contravention by the OES was –

(a) committed with the consent or connivance of, or was attributable to neglect on the part of that person; or

(b) aided, abetted, counselled or procured by that person.

(6) The amount of a penalty imposed under this Article must –

(a) in the opinion of the Minister, be appropriate and proportionate to the contravention in respect of which it is imposed; and

(b) not exceed £10,000.

(7) The Minister may by Order amend the figure in paragraph (6)(b).

37 Appeal against imposition of penalty

(1) An OES may appeal to the Royal Court if it considers that, having regard to the circumstances of the case –

(a) it was unreasonable for the Minister to impose a penalty; or

(b) the amount of the penalty imposed was excessive.

(2) The appeal must be lodged with the Royal Court no later than 28 days after the date of issue of the confirmation notice under Article 36.

(3) If an appeal is lodged, the Minister must not enforce payment of the penalty until the appeal is determined.

(4) The Royal Court may –

(a) confirm the penalty;

(b) rescind the penalty;

(c) substitute a penalty of a different amount; or

(d) make another interim or final order as it sees fit.

38 Contravention by government service

(1) If the Minister becomes aware that a government service is in breach of its security duties under Articles 29, 30 and 32 or its duty to notify the Director of cyber incidents under Article 31, the Minister must take the steps that the Minister, on the advice of the Director, considers necessary.

(2) Those steps may include directing the government service to remedy the breach with the assistance of the Director.

39 Offence: false or misleading information

(1) A person commits an offence if they knowingly or recklessly provide an entitled person with information that is false or misleading in a material particular –

(a) in purported compliance with a requirement under this Law; or

(b) in circumstances in which the person providing the information intends, or could reasonably be expected to know, that the information would be used by the entitled person for the purpose of carrying out their functions under this Law.

(2) A person who commits an offence under paragraph (1) is liable to imprisonment for a term of 5 years and to a fine.

(3) In this Article, "entitled person" means –

(a) the Minister;

(b) the Director;

(c) the JCSC; or

(d) other persons entitled to information under this Law.

(4) A reference to an offence under this Article includes a reference to an offence under Article 1 of the Criminal Offences (Jersey) Law 2009 in relation to that offence.

(5) In paragraphs (6) and (7) –

"relevant offence" means an offence under this Article committed by a limited liability partnership, a separate limited partnership, an incorporated limited partnership or another body corporate;

"relevant person" means –

(a) if the relevant offence is committed by a limited liability partnership, a partner of the partnership;

(b) if the relevant offence is committed by a separate limited partnership or an incorporated limited partnership –

(i) a general partner; or

(ii) a limited partner who is participating in the management of the partnership;

(c) if the relevant offence is committed by a body corporate other than an incorporated limited partnership –

(i) a director, manager, secretary or other similar officer of the body corporate; and

(ii) if the affairs of the body corporate are managed by its members, a member who is acting in connection with the member's functions of management; and

(d) a person purporting to act in any capacity described in sub-paragraphs (a) to (c) in relation to the partnership or body that commits the relevant offence.

(6) If a relevant offence is proved to have been committed with the consent or connivance of a relevant person, that relevant person is also guilty of the offence and liable in the same manner as the partnership or body corporate to the penalty provided for that offence.

(7) A relevant person is guilty of a relevant offence, and liable in the same manner as the partnership or body corporate to the penalty provided for that offence, if the offence –

(a) is an offence that may be committed by neglect; and

(b) is proved to be attributable to neglect on the part of the relevant person.

(8) A fine imposed on an unincorporated association on its conviction of an offence under this Law must be paid out of the funds of the association.

(9) Paragraphs (10) and (11) apply if it is alleged that an offence under this Law has been committed by an unincorporated association (that is, not by a member of the association).

(10) Proceedings for the offence must be brought in the name of the association.

(11) For the purposes of the proceedings, any rules of court relating to the service of documents have effect as if the association were a body corporate (to the extent that those rules do not make specific provision for service on unincorporated associations).

(12) The States may, by Regulations made under Article 41, amend this Article to make alternative or supplementary provision as to liability for offences.

PART 7

INFORMATION SHARING AND CLOSING PROVISIONS

40 Information sharing

(1) A person may disclose information to the Director if the disclosure is made for the purpose of the exercise of a function of the Director.

(2) Information obtained by the Director in connection with the exercise of a function may be used by the Director in connection with the exercise of another function.

(3) The Director may share information with a relevant body if sharing the information is –

(a) necessary –

(i) for the purposes of the Director's functions under this Law;

(ii) in the interests of the security of Jersey; or

(iii) for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution (whether in Jersey or outside Jersey); and

(b) limited to information that is relevant and proportionate to the purpose for which it is shared.

(4) If information is shared under paragraph (3), the relevant body may share the information with another relevant body if –

(a) the conditions in paragraph (3) apply; and

(b) the Director gives consent.

(5) Disclosure under this Article is not to be treated as a breach of a restriction imposed by contract, enactment or otherwise.

(6) In this Article, "relevant body" means –

(a) the States of Jersey Police Force;

(b) the Honorary Police within the meaning of the Honorary Police (Jersey) Law 1974;

(c) the National Crime Agency of the United Kingdom;

(d) a public authority not falling within sub-paragraphs (a) to (c) with functions in part of the British Islands that consist of or include the investigation of crimes or the charging of offenders;

(e) a person with functions in a country or territory outside Jersey that –

(i) correspond to those of a police force; or

(ii) otherwise consist of or include the investigation of conduct contrary to the law of that country or territory, or the apprehension of persons guilty of that conduct; and

(f) a person with functions under an international agreement that consist of or include the investigation of conduct, or the apprehension of persons guilty of conduct, that is –

(i) unlawful under the law of 1 or more places;

(ii) prohibited by an international agreement; or

(iii) contrary to international law;

(g) the CSIRT or SPOC for other countries or territories; or

(h) other persons that the Director considers appropriate.

41 Power to amend this Law by Regulations

(1) The States may, by Regulations, amend this Law (other than this Article) to make alternative or supplementary provision that appears to the States to be appropriate.

(2) This Article does not limit other powers to amend this Law by Regulations or Order.

42 Transitional provisions

(1) The Director of the JCSC on the date of commencement of this Law continues in that position and is treated as having been employed by the States in that capacity beginning with the date of the Director's employment.

(2) A person, other than the Director, employed by or engaged to work for the JCSC before the commencement of this Law is, on its commencement, treated as having been employed or engaged by the States to work in the same capacity beginning with the date of their employment or engagement.

43 Consequential amendments

(1) Schedule 4 contains consequential amendments.

(2) The States may, by Regulations, amend an enactment (other than this Law) to make provisions the States consider necessary or expedient in consequence of the coming into force of this Law, or of an amendment to this Law.

44 Citation and commencement

This Law may be cited as the Cyber Security (Jersey) Law 202- and comes into force on a day to be specified by the Minister by Order.

SCHEDULE 1

(Article 2)

DIRECTOR OF JERSEY CYBER SECURITY CENTRE

1 Appointment and tenure of Director

(1) Other than as set out in this Schedule, the Director holds and vacates office as Director in accordance with the terms and conditions of their appointment.

(2) The Minister must appoint as Director a person who has the appropriate qualifications and experience to fulfil the objectives, carry out the duties and exercise the powers in Part 3.

(3) Before appointing a person as Director the Minister must consult and take into account the views of the Jersey Appointments Commission established under Article 17 of the Employment of States of Jersey Employees (Jersey) Law 2005.

(4) Article 2 of the States of Jersey (Appointment Procedures) (Jersey) Law 2018 applies to the appointment of the Director.

2 Termination of appointment of Director

(1) The Director ceases to hold office –

(a) if the Director resigns by giving notice in writing to the Minister as required under the terms and conditions of their appointment; or

(b) if the Director's appointment is terminated under sub-paragraph (3).

(2) If the Director resigns from office under sub-paragraph (1)(a), the Minister must, as soon as practicable after receiving that notice of resignation, report it to the States Assembly.

(3) The appointment of the Director may be terminated by the Minister if the Director –

(a) is incapacitated physically or mentally from carrying out their functions or is otherwise unable or unfit to discharge their functions;

(b) has been absent from the Director's office for more than 3 months without due cause;

(c) fails, without reasonable excuse, to discharge the Director's duties; or

(d) is disqualified from holding the office of Director under paragraph 3.

(4) Before terminating the appointment the Minister must give notice to the Director.

(5) Article 3 of the States of Jersey (Appointment Procedures) (Jersey) Law 2018 applies to the termination of the Director.

3 Disqualification for appointment, restrictions and exceptions

A person cannot hold the office of Director if the person –

(a) does not hold an appropriate level of security vetting, in the opinion of the Minister;

(b) is not habitually resident in Jersey;

(c) has been convicted of a criminal offence that is sufficiently serious to cast doubt on the Director's suitability to carry out the office; or

(d) has been subject to a finding of gross misconduct at work, whether as Director or in previous employment.

SCHEDULE 2

(Article 4)

CONSTITUTION OF TAC

1 Application of Schedule 2

This Schedule applies to a TAC established under Article 4.

2 Constitution of TAC

(1) The Director must agree with the Minister terms of reference for each TAC.

(2) The Director and the Minister must review the terms of reference at least once every 4 years.

(3) A TAC must consist of at least 3 and no more than 9 members.

(4) A person may be a member of more than 1 TAC.

3 Appointment of members

(1) The Minister must, having received advice from the Director, appoint as members of a TAC people who –

(a) possess the qualifications, skill and experience necessary to perform the functions of a member that are set out in the TAC's terms of reference;

(b) demonstrate a high degree of integrity; and

(c) meet the security clearance requirements set by the Minister and the Director.

(2) Before appointing a person –

(a) the Minister must take advice from the Director about the suitability of the person for the role; and

(b) the Minister may require the person to provide information or references that the Minister reasonably requires to determine the person's suitability for the role.

(3) Each member must be appointed for a term of a minimum of 1 year and a maximum of 3 years, and is eligible for reappointment for a maximum cumulative period of 9 years.

(4) The Director must appoint a chair from among the members.

(5) When appointing a chair the Director must determine the period of the appointment, which must expire before or on the same date as the person's appointment as a member expires.

(6) Unless different provision is made under this Law, a person appointed as chair holds and vacates office in accordance with the terms of their appointment.

(7) The chair must appoint a member as deputy chair, and that person is to be treated as the chair for the purposes of this Law if –

(a) the chair is unable to act through incapacity or absence; or

(b) there is a vacancy in the office of chair.

4 Disqualification for appointment

A person cannot be a member of a TAC if the person does not pass or maintain appropriate security vetting, as set by the Director.

5 Code of conduct

The Minister may suspend a member who, in the Minister's opinion, has failed to uphold the code of conduct, and investigate the matter.

6 Revocation of appointment

(1) The appointment of a member may be revoked by the Minister if –

(a) the member is disqualified for appointment under paragraph 4;

(b) the member has been convicted of a criminal offence that is sufficiently serious to cast doubt on their suitability to carry out the role;

(c) is incapacitated physically or mentally from carrying out their functions or is otherwise unable or unfit to discharge their functions;

(d) the Minister determines, following an investigation under paragraph 5, that the member has failed to uphold the code of conduct; or

(e) the member has been unavailable for contact by any member of the TAC for more than 3 months without due cause.

(2) Before revoking the appointment of a member, the Minister must –

(a) give the Director and the member notice of the Minister's intention to revoke the appointment; and

(b) give the member an opportunity to make representations to the Minister regarding the proposed revocation (except for revocation under sub-paragraph (1)(a)).

(3) If the Minister revokes the appointment of a member, the Minister must inform the Director and the relevant TAC as soon as practicable.

7 Remuneration of members

The Minister must determine the remuneration, if any, of the members.

SCHEDULE 3

(Article 22)

ESSENTIAL SERVICES, THRESHOLD REQUIREMENTS AND CONDITIONS

PART 1

ENERGY SECTOR

1 Electricity subsector

(1) For the essential service of importing electricity, the threshold requirement is that the person imported 150 megawatt hours of electricity into Jersey in the previous financial year, for delivery to final customers.

(2) For the essential service of generating electricity, the threshold requirement is that the person generated 150 megawatt hours of electricity in the previous financial year, for delivery to final customers.

(3) For the essential services of transmitting and distributing electricity, the threshold requirement is that the person operates a transmission system or a distribution system that –

(a) served at least 10,000 final customers in the previous financial year; or

(b) has the potential to disrupt delivery to at least 10,000 final customers.

(4) For the essential service of selling electricity, the threshold requirement is that the person sold electricity to at least 10,000 final customers in the previous financial year.

(5) In this paragraph –

"distribution system" means a system that consists wholly or mainly of low-voltage lines and electrical plant used for conveying electricity for delivery to final customers;

"final customer" means a person in Jersey purchasing electricity for their own use;

"transmission system" means a system that consists wholly or mainly of high-voltage lines and electrical plant used for conveying electricity for delivery to final customers or distributors.

2 Crude oil based fuel subsector

(1) For the essential service of importing crude oil based fuel, the threshold requirement is that the person imported at least 5,000,000 litres of crude oil based fuel into Jersey in the previous financial year.

(2) For the essential service of storing crude oil based fuel, the threshold requirement is that the person operates a facility or facilities with a total capacity of at least 5,000,000 litres of crude oil based fuel.

(3) For the essential service of supplying crude oil based fuel, the threshold requirement is that the person delivered at least 5,000,000 litres of crude oil based fuel to final customers, or to retail sites for delivery to final customers, in the previous financial year.

(4) For the essential service of supplying crude oil based fuel, the threshold requirement is that the person supplied at least 5,000,000 litres of crude oil based fuel to final customers in the previous financial year.

(5) In this paragraph –

"crude oil" means liquid hydrocarbon mixture occurring naturally in the earth whether or not treated to render it suitable for transportation, and includes –

(a) crude oils from which distillate fractions have been removed; and

(b) crude oils to which distillate fractions have been added;

"crude oil based fuel" means fuel wholly or mainly made up of crude oil or substances derived from crude oil;

"final customer" means a person in Jersey purchasing crude oil based fuel for their own use.

3 Gas subsector

(1) For the essential service of importing liquid petroleum gas ("LPG"), the threshold requirement is that the person imported 900,000 cubic metres of LPG into Jersey in the previous financial year, for delivery to final customers.

(2) For the essential service of storing LPG, the threshold requirement is that the person operates a facility with a total capacity of at least 3,000 cubic metres of LPG.

(3) For the essential service of distributing mains gas, the threshold requirement is that the person delivered gas, by the mains gas network –

(a) to at least 2,000 final customers in the previous financial year; or

(b) with a potential to disrupt delivery to at least 2,000 final customers.

(4) For the essential service of distributing LPG, the threshold requirement is that the person delivered LPG to at least 2,000 final customers in the previous financial year.

(5) For the essential service of selling mains gas or LPG, the threshold requirement is that the person sold mains gas or LPG to at least 2,000 final customers in the previous financial year.

(6) In this paragraph –

"final customer" means a person in Jersey purchasing LPG or mains gas for their own use;

"mains gas" means gas suitable to be delivered by the mains gas network;

"mains gas network" means the mains, pipes and other apparatus by which mains gas may be delivered to final customers.

PART 2

TRANSPORT SECTOR

4 Sea transport subsector

(1) For the essential service of carrying out harbour operations, the condition is that the person is licensed under Part 3 of the Air and Sea Ports (Incorporation) (Jersey) Law 2015 to carry out harbour operations.

(2) In this paragraph, "harbour operations" has the meaning given in Article 2(3) of the Air and Sea Ports (Incorporation) (Jersey) Law 2015.

5 Air transport subsector

(1) For the essential service of carrying out airport operations, the condition is that the person is licensed under Part 3 of the Air and Sea Ports (Incorporation) (Jersey) Law 2015 to carry out airport operations.

(2) In this paragraph "airport operations" has the meaning given in Article 2(2) of the Air and Sea Ports (Incorporation) (Jersey) Law 2015.

6 Freight handling subsector

For the essential service of freight handling, the threshold requirement is that the person loaded or unloaded a total of at least 100,000 tonnes of freight at Jersey ports in the previous financial year.

7 Road transport and freight distribution subsector

For the essential service of transporting freight by road to and from Jersey ports, the threshold requirement is that the person transported at least 100,000 tonnes of freight in the previous financial year.

PART 3

FINANCIAL SERVICES SECTOR

8 Banking subsector

For the essential service of providing banking services, the condition is that the person is registered under Part 2 of the Banking Business (Jersey) Law 1991 and regulated by the JFSC.

PART 4

HEALTH SECTOR

9 Medical services subsector

The following are essential services –

(a) Health services carried on at, or operating out of, a hospital;

(b) "Hospital" means premises, other than at the prison (as defined in Article 1 of the Prison (Jersey) Law 1957) –

(i) used for the reception and inpatient treatment of people suffering from illness or injury;

(ii) used for the reception and inpatient treatment of people during convalescence or people requiring medical rehabilitation; or

(iii) maintained in connection with premises described in clauses (a) or (b) and used as –

(A) a clinic;

(B) a dispensary; or

(C) a department treating outpatients (whether or not the department also treats inpatients).

PART 5

WATER SECTOR

10 Drinking water supply subsector

(1) For the essential service of supplying drinking water, the threshold requirement is that the person supplied mains water to at least 10,000 final customers in the previous financial year.

(2) In this paragraph –

"final customer" means a person in Jersey purchasing mains water for their own use;

"mains water" means drinking water supplied to final customers via a main (as defined in Article 1 of the Water (Jersey) Law 1972).

PART 6

DIGITAL SECTOR

11 Public communications subsector

(1) For the essential service of providing public communications, the condition is that the person –

(a) is a public communications provider;

(b) provides a service to customers in Jersey;

(c) holds a licence under the Telecommunications (Jersey) Law 2002 that is designated as a Class II or Class III licence by the JCRA; and

(d) has a place of business, office or staff in Jersey.

(2) In this paragraph –

"public communications provider" means –

(a) a provider of a public electronic communications network;

(b) a provider of a public electronic communications service; or

(c) a person who makes available facilities that are associated facilities by reference to a public electronic communications network or a public electronic communications service;

"public electronic communications network" means an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public;

"public electronic communications service" means an electronic communications service that is provided to be available for use by members of the public.

12 Digital services subsector

(1) For the essential service of providing information and communications technology services, the condition is that the person, by providing assistance or active administration carried out either on customers' premises or remotely, provides services –

(a) related to the installation, management, operation or maintenance of information and communications technology products, networks, infrastructure, applications or other network and information systems; and

(b) to another OES in Jersey.

(2) For the essential service of providing a managed security service provider, the condition is that the person –

(a) provides a managed service that carries out or assists with activities relating to cyber security risk management; and

(b) is based in Jersey.

(3) For the essential service of providing cloud computing services, the condition is that the person is based in Jersey.

(4) For the essential service of providing a data centre service, the condition is that the person is based in Jersey.

(5) In this paragraph –

"cloud computing service" means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including situations in which those resources are distributed across more than 1 location;

"digital service" means a service that is provided –

(a) for remuneration;

(b) at a distance;

(c) by electronic means; and

(d) at the request of the recipient of the service.

13 Operator of the .je domain name subsector

The person assigned as the designated manager for the .je domain name by the Internet Assigned Numbers authority or a successor organisation is an operator of an essential service.

14 Domain name services subsector

(1) For the essential service of providing domain name registration services, the threshold requirement is that the person registers domain names on behalf of other people operating in Jersey, if –

(a) 100 or more domain names are registered and in active use; or

(b) a domain name is registered by an OES and is in active use.

(2) For the essential service of providing DNS services, the threshold requirement is that the person provides authoritative DNS for domain names used by other people operating in Jersey, if those services –

(a) are provided for 100 or more domain names in active use; or

(b) are provided for a domain name in active use by an OES.

(3) In this paragraph –

"authoritative DNS" means a service for holding and distributing the definitive records of a particular domain name;

"in active use" means the domain name is used other than for indicating that it is registered and may be available for sale.

PART 7

POSTAL AND COURIER SERVICES SECTOR

15 Postal service subsector

A postal service (as defined in Article 1(1) of the Postal Services (Jersey) Law 2004) provided by Jersey Post International Limited or a subsidiary of that company is an essential service.

16 Courier services subsector

(1) For the essential service of providing courier services, the threshold requirement is that the person delivered at least 10,000 items of mail in the previous financial year.

(2) In this paragraph, "mail" has the meaning given in Article 1(1) of the Postal Services (Jersey) Law 2004.

17 Couriers of necessary supplies subsector

(1) For the essential service of courier of necessary supplies, the threshold requirement is that the person delivered necessary supplies to or within Jersey in the previous financial year.

(2) "Necessary supplies" are –

(a) medical supplies (as defined in Article 8A of the Emergency Powers and Planning (Jersey) Law 1990);

(b) other supplies prescribed by the Minister by Order.

PART 8

FOOD SECTOR

18 Food production subsector

Jersey Dairy Limited is an essential service.

19 Food retail subsector

(1) For the essential service of food retail, the threshold requirement is that the person –

(a) places food on the market; and

(b) operates a shop –

(i) that is a single premises with a retail sales area of 700 square metres or more; and

(ii) in which at least 50% of the retail sales area is given over to the sale of food.

(2) In this paragraph –

"food" means a substance or product, whether processed, partially processed or unprocessed that is intended to be, or reasonably expected to be, ingested by humans; and includes –

(a) drink;

(b) chewing gum;

(c) a substance, including water, intentionally incorporated into the food during its manufacture, preparation or treatment; and

(d) water that –

(i) in the case of water supplied from a distribution network, is after the point within premises at which it emerges from the taps that are normally used for human consumption;

(ii) in the case of water supplied from a tanker, is after the point at which it emerges from the tanker;

(iii) in the case of water put into bottles or containers intended for placing on the market, is after the point at which the water is put into the bottles or containers; or

(iv) in the case of water used in a food production undertaking, is after the point where the water is used in the undertaking;

but "food" does not include –

(a) a substance or product, including additives, whether processed, partially processed or unprocessed, intended to be used for oral feeding to animals;

(b) live animals, unless they are prepared for placing on the market for human consumption;

(c) plants prior to harvesting;

(d) medicinal products within the meaning of Article 2 of the Medicines (Jersey) Law 1995;

(e) cosmetic products, being a substance or mixture intended to be placed in contact with the external parts of the human body or with the teeth and the mucous membranes of the oral cavity with a view exclusively or mainly to cleaning them, perfuming them, changing their appearance, protecting them, keeping them in good condition or correcting body odours;

(f) tobacco and tobacco products within the meaning of Article A1 of the Restriction on Smoking (Jersey) Law 1973;

(g) narcotic substances within the meaning of the United Nations Single Convention on Narcotic Drugs signed at New York on 30 March 1961, or psychotropic substances within the meaning of the United Nations Convention on Psychotropic Substances, 1971;

(h) residues or contaminants in or on food;

"places on the market" in relation to food means –

(a) the holding of food for the purpose of sale, including offering for sale or another form of transfer, whether on payment of money or not; or

(b) the sale, distribution or other form of transfer of food;

"retail sales area" has the meaning given in Article 2 of the Shops (Regulation of Opening) (Jersey) Regulations 2011.

PART 9

PUBLIC ADMINISTRATION SECTOR

20 Parishes and public bodies subsector

The following are essential services –

(a) a parish of Jersey;

(b) an organisation specified in Schedule 2 to the Public Finances Law;

(c) the JFSC;

(d) the JCRA;

(e) the Data Protection Authority established under Article 2 of the Data Protection Authority (Jersey) Law 2018; and

(f) the Jersey Heritage Trust incorporated by an Act of Incorporation granted by the States by the Loi accordant un Acte d'Incorporation à l'Association dite "The Jersey Heritage Trust" registered on 3 June 1983.

21 Emergency services subsector

The following are essential services –

(a) States of Jersey Police Force;

(b) Ambulance service carried out by people employed under the Employment of States of Jersey Employees (Jersey) Law 2005 for that purpose;

(c) States of Jersey Fire and Rescue Service continued under Article 3 of the Fire and Rescue Service (Jersey) Law 2011;

(d) Airport Rescue and Firefighting Service, as defined in Article 1 of the Fire and Rescue Service (Jersey) Law 2011.

SCHEDULE 4

(Article 43)

CONSEQUENTIAL AMENDMENTS

1 Computer Misuse (Jersey) Law 1995

After Article 5A of the Computer Misuse (Jersey) Law 1995 there is inserted –

5B Exemption for cyber security

Articles 2, 5 and 5A do not apply to –

(a) the Director of the Jersey Cyber Security Centre appointed under Article 2 of the Cyber Security (Jersey) Law 202- or a person employed by and working under the full operational control of the Director, if the conduct in question was undertaken –

(i) in good faith; and

(ii) in the course of the person's employment duties;

(b) the Minister for Sustainable Economic Development, to the extent that the Minister is discharging a function under the Cyber Security (Jersey) Law 202-.

2 Data Protection (Jersey) Law 2018

(1) This paragraph amends the Data Protection (Jersey) Law 2018.

(2) In Article 41 –

(a) in paragraphs (2), (5) and (9), "for Justice and Home Affairs" is deleted;

(b) after paragraph (1) there is inserted –

(11) In this Article, "Minister" means –

(a) the Minister for Sustainable Economic Development, if the matter relates to the discharge of that Minister's functions under the Cyber Security (Jersey) Law 202-;

(b) in any other case, the Minister for Justice and Home Affairs.

(3) In Schedule 1, paragraph 1, after "Jersey Customs & Immigration Service" there is inserted "Jersey Cyber Security Centre".

3 Emergency Powers and Planning (Jersey) Law 1990

For Article 6 of the Emergency Powers and Planning (Jersey) Law 1990 there is substituted –

6 Powers of competent authority in relation to telecommunications, cyber security and cyber resilience

(1) A competent authority may by Order provide for securing, regulating or prohibiting 1 or more of the following –

(a) telecommunication services, telecommunication systems and apparatus, cyber network and information systems and operational technology;

(b) the use of those services, systems, networks, apparatus and technology.

(2) A competent authority may by Order provide for regulating the price at which those services, systems, networks, apparatus and technology may be supplied.

(3) A provision made by Order under this Article may –

(a) be made either –

(i) in relation to telecommunication services, telecommunication systems and apparatus, cyber network and information systems and operational technology in general; or

(ii) in relation to a particular description of those services, systems, networks, apparatus and technology; and

(b) be made –

(i) with respect to the supply, distribution, acquisition or use of the things referred to in sub-paragraph (a)(i) or described in sub-paragraph (a)(ii);

(ii) for a particular purpose specified in the Order; or

(iii) for all purposes.

(4) An Order under this Article may empower a competent authority to give directions to –

(a) persons carrying on business as a provider of telecommunication services, telecommunication systems or apparatus, or cyber network and information systems or operational technology, about the provision of those things;

(b) a person carrying on business involving the use of those things, about the person's use of those things for the purposes of that business.

(5) A competent authority may by Order make provision for suspending, modifying or excluding a contractual obligation, or an obligation or restriction imposed by or under an enactment, that directly or indirectly affects the provision or use of telecommunication services, telecommunication systems or apparatus, or cyber network and information systems or operational technology, or for extending a power conferred by such an enactment.

(6) In this Article –

"apparatus", "telecommunication service" and "telecommunication system" have the same meanings as in the Telecommunications (Jersey) Law 2002;

"cyber network and information system" has the same meaning as "network and information system" as defined in Article 1 of the Cyber Security (Jersey) Law 202-;

"operational technology" has the same meaning as in Article 1 of the Cyber Security (Jersey) Law 202-.

4 Freedom of Information (Jersey) Law 2011

In Article 26A(2) of the Freedom of Information (Jersey) Law 2011, after sub-paragraph (o) there is inserted –

(p) the Director appointed under Article 2 of the Cyber Security (Jersey) Law 202-;

(q) an employee of the JCSC employed under that Article;

(r) the Minister for Sustainable Economic Development, to the extent that the Minister is discharging a function under that Law.

5 Telecommunications (Jersey) Law 2002

In the Telecommunications (Jersey) Law 2002 –

(a) in Article 24U(4), before sub-paragraph (a) there is inserted –

(aa) the JCSC appointed under Article 2 of the Cyber Security (Jersey) Law 202-;

(ab) the Director of the JCSC appointed under that Article;

(ac) the Minister for Sustainable Economic Development, to the extent that the Minister is discharging a function under the Cyber Security (Jersey) Law 202-;