Economy

Consultation on proposed Cyber Defence legislation

16 DECEMBER 2022

Consultation Paper:

Contents

Background

1.1 As part of Jersey's efforts to be cyber resilient the Council of Ministers agreed the establishment of the Cyber Emergency Response Team (CERT.JE). This was a key recommendation in the 2017 Cyber Security Strategy. The creation of a cyber emergency response capability is integral to strengthening Jersey's national cyber resilience and international reputation and vital for the continued growth and development of Jersey's economy.

1.2 Since June 2021, the Cyber Emergency Response Team for Jersey (CERT.JE) has operated within the Department for the Economy and has been funded as part of the Government Plan. The remit of CERT.JE is broader than just providing a response in a cyber emergency and it has been agreed that the more appropriate name should be The Cyber Security Centre for Jersey (CSCJ).

1.3 The Cyber Security Centre for Jersey will become an independent advisory and emergency response body and is the intention for The Cyber Security Centre for Jersey to operate at arm's length from regulators, law enforcement officers and government as a grant funded body.

1.4 The goal of The Cyber Security Centre for Jersey is to *prepare for, protect against, and respond to* cyber attacks on Jersey. The Cyber Security Centre for Jersey will engage and communicate with industry, public bodies and the third sector as well as develop clear standards, expectations and support for cyber security risk management, control and assurance (*protect against*) and have the ability to monitor threats to the island and respond to major incidents (*respond to*). This will provide the island with a balanced approach

that enables the cyber risk profile of the island to be reduced over time, whilst providing a proactive service to reduce the significant cyber security risks the island faces.

1.5 It is the policy intent that the services and functions provided by The Cyber Security Centre for Jersey are aligned with globally recognised services and functions provided by other national cyber emergency centres. Therefore, it is expected that The Cyber Security Centre for Jersey will follow the recognised service framework as detailed by the Forum of Incident Response and Security Team (FIRST.org), a global network of cyber security centres and specialists. This service framework, called the Computer Security Incident Response Team (CSIRT) Services Framework, has been reviewed by cyber security experts and is supported by from the Task Force CSIRT (TF-CSIRT) Community, and the International Telecommunications Union (ITU).

1.6 In order to establish The Cyber Security Centre for Jersey, legislation needs to be put in place outlining the scope of the work expected of The Cyber Security Centre for Jersey and the governance around the work which is the scope of this consultation.

Section A: Remit and Functions of The Cyber Security Centre for Jersey

A1. The remit of The Cyber Security Centre for Jersey captures the activities the team would be expected to deliver against to help enable delivery of Government and Ministerial priorities relevant to cyber security. The listed functions, detailed in paragraph A3 are those activities that will be referenced in the new piece of legislation.

A2. As detailed in the Background section, it has been agreed that the following areas fall within the remit of The Cyber Security Centre for Jersey:

i. Information Security Event Management. This means monitoring threat intelligence (global information on internet and computer activity that may indicate a threat or risk to Jersey), analysing this information and undertaking a triage process to prioritise it and determine where action is appropriate in order to prepare, protect or defend the constituency from cyber threats.

ii. Information Security Incident Management. This means receiving intelligence on security incidents (including from the process above) and actioning them appropriately. This would include analysis, categorisation and prioritisation of the incident, recommending, supervising, contributing to or undertaking analysis and forensic analysis of relevant technical artefacts (such as laptops, mobile devices, suspected malware, or internet traffic), recommending or undertaking mitigation and recovery actions, coordinating incident response locally or internationally, and providing support for crisis management - this could include, for example, advising or undertaking communications with the public or engagement/negotiation with criminal hackers.

iii. Vulnerability Management. A vulnerability is a weakness in an information system that could potentially be exploited. A vulnerability can be technical, process related, or human behaviour related. This service would include discovery of vulnerabilities through both proactive research, and through notification by others including security researchers (sometimes referred to as 'hackers') and users of systems. Receipt of vulnerability reports, analysis of vulnerabilities, coordination of response, for example with impacted organisations or technology providers), disclosure of the vulnerability (for example to other CERTs/CSIRTs, the technology providers or national security agencies, or to users of the systems), and response, including recommending and communicating ways to resolve the vulnerability or mitigate the risk.

iv. Situational Awareness. This means building and maintaining a clear picture of global cyber security threats and how these apply to CERT.JE's constituency. It includes acquisition of data (for example from news sources, technical data feeds, industry intelligence, national security information, and direct industry engagement), analysis and synthesis of this information to identify actionable insights relevant to Jersey (for example, knowledge of a particular systems vulnerability combined with knowledge of a threat actor using similar vulnerabilities, combined with knowledge that we operate such systems in Jersey, would allow us to predict a threat and address the risk before any impact is felt locally), and communication of this information, both in order to drive immediate behaviours, and to drive longer term change and priorities, for example through the Island Wide Cyber Risk Assessment or threat specific risk assessments (such as that carried out for Operation Calcite, our response to Russia's invasion of Ukraine)

v. Knowledge Transfer. This includes raising awareness of cyber security risks and threats, training and educating residents and organisations in the nature of these threats and how to respond to them effectively, and advising organisations on effective mitigation strategies. This would also include the provision of best practices and guidance on, for example, how organisations should develop incident response plans, undertake cyber risk assessments, or implement appropriate steps to secure systems and data.

vi. Promote and enable cyber security information sharing amongst organisations to ensure awareness of existing threats and to provide the ability to take prompt action either on an organisational or island-wide basis. This may be through provisions to ensure information sharing (for example, incidents affecting operators of essential services which may impact island resilience), or through voluntary information sharing.

vii. Increase the level of cyber resilience across the Island. In collaboration with the of Government of Jersey, Critical National Infrastructure and business communities to reduce the risk and impact of major cyber incidents. This may include, for example, provision of support services to relevant organisations (either funded through budget or through cost recovery / cost sharing), setting appropriate standards for cyber security (with the endorsement of Government and through consultation and agreement with relevant competent authorities), through international engagement and cooperation, and through support to boards and stakeholders.

viii. Represent Jersey's cyber security interests locally and internationally, within international cyber security bodies and in dealings with other cyber-attack expertise and response centres. This aligns with the role of the UK National Cyber Security Centre and other national cyber emergency response teams.

ix. Uphold Jersey's cyber security reputation by ensuring Jersey meets the appropriate international standards of best practice for cyber security, obtaining and maintain appropriate recognition as a national cyber security agency within the context of a Crown Dependency

x. Maintain oversight of and report independently on the cyber risk posture of the Island and constituency, for example by undertaking cyber risk assessments for the purposes of CERT.JE, on behalf of Government of Jersey, and to facilitate Resilience/Emergency Planning.

xi. Support and enable effective cyber capability across public services and agencies, for example working with and supporting Regulators, Law Enforcement and Government (including with advice, services, expertise and capacity) without prejudice to The Cyber Security Centre for Jersey's role as an independent trusted advisor.

xii. Operate within appropriate and proportional governance, that protects The Cyber Security Centre for Jersey's need for operational independence whilst at the same time respecting it's public mandate. Operate in a financially fiscally responsible manner to deliver against Government policy and Ministerial priorities.

A3. The new cyber defence legislation will define some of the functions of The Cyber Security Centre for Jersey. Namely:

a. monitoring incidents in Jersey; including having the powers to scan publicly accessible networks and systems for malicious activity ('indicators of compromise'), vulnerabilities or configuration errors

b. providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;

c. respond appropriately to any incident notified to it by any person. Private sector business, government department etc.;

d. provide risk and incident analysis and situational awareness;

e. participate and co-operate in the wider cyber security network;

f. establish relationships with the private sector in order to facilitate co-operation with that sector;

g. promote the adoption of and use of common or standardised practices for—

    i. cyber risk management

    ii. cyber security

    iii. incident and risk handling procedures, and

    iv. incident, risk and information classification schemes;

h. co-operating with enforcement authorities to enable the enforcement authorities to fulfil their obligations

i. facilitate disclose of and receive information from any person if the disclosure is made for the purposes of exercise of any The Cyber Security Centre for Jersey function

j. share information as necessary and appropriate with law enforcement, other cyber emergency response teams, and national security bodies, without obtaining permission from data subjects and without restriction as to commercial contracts, as long as it is shared for the purposes of exercise of any The Cyber Security Centre for Jersey function

k. provide or co-ordinate delivery of cyber security services on behalf of local organisations (for example to support shared delivery of security operations, incident response, of vulnerability disclosure services on behalf of multiple organisations).

l. maintain the confidentiality of information, including entering into MOUs and data sharing agreements, and ensuring non-disclosure of information to regulators, government or law enforcement except under court order.

m. for the purposes of agreed functions and with the appropriate permission or at the request of the States of Jersey Police, Jersey Office of the Information Commissioner, Jersey Financial Services Commission, or Jersey Competition Regulatory Authority interrogate computers and networks without liability;

n. only when necessary or appropriate for delivery against the agreed purpose and functions collect and process malware and intelligence including content that may be illegal to access, store or distribute (e.g. accessing dark web);

o. adopt or set guidance and standards in cyber security for Jersey. When setting standards, The Cyber Security Centre for Jersey should follow due process and consultation and engage with Government of Jersey and other relevant stakeholders to ensure the standards are recognised, appropriate and proportionate for Jersey The final standard should be approved by the Board before publication.

p. carry out incident readiness and response exercises with participation from public bodies;

q. give the Government of Jersey, telecommunications operators and Critical National Infrastructure organisations the right to share information with The Cyber Security Centre for Jersey about cyber security events when this information might otherwise be subject to restriction ; or

r. issue Guidance including general advice, and Notices (including urgent advice in response to a specific issue or vulnerability) which should be taken into account by public bodies;

Section A: Remit and Functions

1. Do you consider the remit of the Cyber Security Centre for Jersey to be sufficiently broad enough to help increase the cyber resilience of Jersey, please explain your response?
2. Do you feel anything should be added or omitted to the remit of the Cyber Security Centre for Jersey, please explain your response?
3. Do you consider the legal functions provided to the Cyber Security Centre for Jersey are sufficiently broad enough to enable the operation of a national cyber defence capability for Jersey?
4. The Cyber Security Centre for Jersey is not to be a regulator, and this is reflected in both the remit and functions. Do you agree with this, please explain your response?

Section B: Area of operation

B1. The Cyber Security Centre for Jersey has a defined operational mandate for Jersey. The defined Jurisdiction of Jersey includes:

a. all organisations established within the jurisdiction, including the States of Jersey, public sector organisations, private companies, charities and third sector organisations,

b. critical national infrastructure providers operating services in Jersey (regardless of domicile);

c. individuals resident in Jersey;

d. the .JE top level domain name (gTLD); and/or

e. services using telephone and IP ranges allocated to Jersey telecoms providers or for use in Jersey. Effectively, this reflects where cyber incidents would lead to reputational, political, economic or wellbeing risks to the Island or Islanders. It is anticipated that legislation will provide sufficient remit to deliver to this scope.

Section B: Area of operation.

5. Do you consider the operational mandate within the defined Jurisdiction of Jersey to be sufficiently broad enough, please explain your response?

Section C: Governance of The Cyber Security Centre for Jersey

Appointment of the Chief Executive Officer

C1. The Chief Executive Officer of The Cyber Security Centre for Jersey must be appointed by the Minister. The Minister must have regard to the qualifications, experience and necessary skills to perform the role.

C2. The Minister will be given the power to vary or terminate the terms of the appointment, in consultation with the governance Board.

C3. The Chief Executive Officer is responsible for ensuring The Cyber Security Centre for Jersey exercises its functions effectively; proportionally to threats and risks to Jersey from cyber incidents and in accordance with the present international standards on preventing and combating cyber threats, cyber incidents and cyber crime.

C4. The Chief Executive Officer must make reasonable efforts to ensure that the employees of The Cyber Security Centre for Jersey maintain high professional standards, are of high integrity and appropriately skilled and trained and have the appropriate security clearance levels for handling and disseminating sensitive and confidential information.

Establishment of a Governance Board

C5. A Board will be established to ensure the effective governance of The Cyber Security Centre for Jersey. The role of the Board is to provide support and constructive challenge to the Chief Executive Officer and to support and promote the work of The Cyber Security Centre for Jersey and cyber resilience in Jersey - both locally and internationally.

C6. The Chair of the Board will be appointed by the Minister who must have regard to the need to ensure that the Chair has absolute unquestionable integrity, the qualifications, experience and skills necessary to exercise and perform the functions of the Chair. The Chair should not be the Chief Executive Officer, an employee of The Cyber Security Centre for Jersey or a Government employee. The Chair will be a voting member of the Board.

C7. The Board will comprise of a minimum of two voting members, with

a. at least one representative as a voting member with a significant professional background in cyber security, and current qualifications equal or equivalent to the standard set by the UK Cyber Security Council for a Chartered Security Professional, or the Institute of Information Security for a Full Member;

b. one non-voting representative from a Government department making sure that there is always a majority of the Board which is independent of Government;

c. the Chief Executive Officer as a non-voting member and

d. at least one other independent voting Board member.

C8. In the event of equality in the votes of the other voting members present, the Chair will exercise a casting vote. In the event that the Chair is not present, the person elected to Chair the Board meeting must be selected from the voting members present.

C9. The maximum term for any voting Board member shall be 7 years. The Chief Executive Officer shall make recommendations to the Minister on appointments, with the Minister having the final decision.

Sub-Committees

C10. In order to maximise opportunities for inclusion and working in partnership with other organisations, the Board shall have the power to determine if a sub-committee should be set up. The establishment of any sub-committee would be to provide oversight and support the delivery of The Cyber Security Centre for Jersey's functions. Any sub-committee may comprise of persons who are not members of the Board.

C11. Any sub-committee established would be required to provide progress reports to the Board at least twice a year and upon request of the Board with no less than 28 days notice.

Section C: Governance

6. Do you have any comments regarding the current proposals regarding the appointment and governance of The Cyber Security Centre for Jersey?
7. Do you consider the proposed structure of the Board is sufficient to provide effective governance of The Cyber Security Centre for Jersey, please explain your answer?

Section D: Reporting requirements of The Cyber Security Centre for Jersey

D1. For the preceding year, the Chief Executive Officer of The Cyber Security Centre for Jersey will provide annually to the Board and to the Minister:

a. a report on the activities and effectiveness of The Cyber Security Centre for Jersey and on any other matters relevant to the exercise of the functions of The Cyber Security Centre for Jersey that the Chief Executive Officer of considers appropriate;

b. a financial report setting out details of the expenditure of The Cyber Security Centre for Jersey ;

c. the number and nature of mandatory incidents notified to The Cyber Security Centre for Jersey.

D2. There is no requirement for information to be shared where it contains confidential information or information which might prejudice the security or commercial interests of those providing information, crime prevention and national security.

D3. Reports are to be provided as soon as practicable after the end of the financial year and in any event within 4 months of the end of the calendar year. These reports are to be made public.

D4. For your information, as a grant funded body The Cyber Security Centre for Jersey will be required to adhere to the Public Finance Manual in relation to annual reporting.

Section D: Reporting requirements of The Cyber Security Centre for Jersey

8. As The Cyber Security Centre for Jersey will be a grant funded body, are you satisfied with this level of annual reporting. Please explain your answer?

Section E: Sharing Information

E1. The Cyber Security Centre for Jersey will have the power to share information with other, relevant law-enforcement authorities and public authorities where in the view of the Chief Executive Officer, that information sharing is beneficial for—

a. the performance of any functions of an enforcement authority under or by virtue of any future Regulations or any other enactment;

b. national security purposes; or

c. purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution;

E2. The information which may be shared by The Cyber Security Centre for Jersey shall be limited to information which is relevant and proportionate to the purpose of the information sharing.

E3. When sharing information with a public authority or an enforcement authority The Cyber Security Centre for Jersey will not be required to share

a. confidential information, or

b. information which may prejudice the security or commercial interests of operators of essential services or digital service providers.

E4. The power to share information requested will be operable immediately on the receipt of information in circumstances where The Cyber Security Centre for Jersey considers that it is critical or necessary to share that information. The rationale for this is that cyber attacks by their nature happen unexpectedly and dangerous situations can develop rapidly and there is a need to react and intercept quickly.

E5. Any person or entity shall be able to disclose information in a real time situation to The Cyber Security Centre for Jersey, without the necessity of following a legal process. Without the ability to act fast, the cyber threat may exacerbated. This will enable the Cyber Security Centre for Jersey to respond to incidents quickly, to reduce to overall cyber security risk to Jersey.

E6. In order for The Cyber Security Centre for Jersey to carry out its functions it will be exempt from Freedom of Information requests and some for the data subject rights under the Data Protection (Jersey) Law 2018. For transparency, due to these exemptions, The Cyber Security Centre for Jersey will publish an annual report which will maintain the confidentiality of information shared.

Section E: Information Sharing

9. Are there any areas of concern with the information sharing provision afforded to The Cyber Security Centre for Jersey, please explain your response?

Section F: Definitions to be used in legislation

F1. As with all primary legislation in Jersey, key definitions will be defined in an Interpretation section at the beginning of the legislation. The proposed definitions are below, for information purposes some of the proposed definitions mirror UK legislation and it is considered appropriate to use internationally understood terminology where possible.

i. "Board" means The Cyber Security Centre for Jersey Governance Board established under the new legislation

ii. "CERT.JE" means the Jersey Cyber Emergency Response Team which is The Cyber Security Centre for Jersey.

iii. "cyber security incident" means a breach or threat of an imminent breach of a system's security policy in order to affect its confidentiality or integrity or availability and/or the unauthorised access or attempted unauthorised access to a system or systems;

iv. "digital service provider" means any person or organisation who provides a digital service;

v. "financial year" means financial year of The Cyber Security Centre for Jersey, being the period beginning with the day on which Article 2 comes into force and ending with 31st December in the following year, and each subsequent period of 12 months ending with 31st December in each year;

vi. "function" includes power, authority and duty;

vii. "GCHQ" means the UK Government Communications Headquarters within the meaning of section 3 of the Intelligence Services Act 1994";

viii. "incident" means any event having an actual adverse effect on the security of network and information systems;

ix. "Minister" means the Minister for Economic Development, Tourism, Sport and Culture;

x. "network and information system" ("NIS") means—

a. a transmission system for the conveyance, by the use of electrical, magnetic or electro-magnetic energy, of signals of any description and such of the following as are used, by the person providing the system and in association with it, for the conveyance of the signals including-

(i) apparatus comprised in the system;
(ii) apparatus used for the switching or routing of the signals;
(iii) software and stored data and
(iv) other resources, including network elements which are not active;

b. any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

c. digital data stored, processed, retrieved or transmitted by elements covered under paragraph (a) or (b) for the purposes of their operation, use, protection and maintenance";

xi. "operator of an essential service" ("OES") means a person or organisation who is deemed to provide an essential service for the Jurisdiction of Jersey. Identification of essential services are as follows:

a. an entity providing a service essential for the maintenance of critical societal and/or economic activities;

b. the provision of the service depends on network and information systems;

c. and an incident would have significant disruptive effects on the provision of that service

d. For example, these services for Jersey would include:

Table 1: Operators of Essential Services within Jersey

Sector	**Subsector**	**Provider of Service**
Energy	Electricity	Distributors of for Jersey, for example Jersey Electricity
	Oil	Distributors of for Jersey
	Gas	Distributors of for Jersey, for example Island Energy
Transport	Air and Water	Providers serving Jersey covering harbours, marinas, coast guard and airport, for example Ports of Jersey
Banking and Financial Service Providers		Those registered with Jersey Financial Services Commission (JFSC)
Health	Care providers	All public and private health care providers
Drinking water	Supplier and distributor of	Providers serving Jersey, for example Jersey Water
Waste Water		Government of Jersey
Digital Infrastructure	Telecoms providers	All telecoms providers serving Jersey
	Providers of Information and Network Services	Jersey infrastructure providers, web providers, .je domain registers
Public Administration	Parishes	All services offered by Parishes
	Island wide	Government of Jersey
Postal services		Providers serving Jersey for example Jersey Post
Food production, processing and distribution		Key retail and food service operators Major grocery providers of essential products
Jersey based Regulators		Regulators for Jersey, for example: Jersey Financial Services Commission (JFSC) Jersey Office of the Information

		Commissioner (JOIC) Jersey Competition Regulatory Authority (JCRA) Jersey Gambling Commission

xii. "risk" means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems.

xiii. "single point of contact" ("SPOC") as explained in Section E;

xiv. "sub-committee committee" means a committee set up by the Board

Section F: Definitions to be used in legislation

10. Are the definitions explained in sufficient detail, please explain your response?
11. Is the definition of an 'Operator of an Essential Services' broad enough to capture services that if suffered a cyber security incident would impact societal and/or economic activities on Jersey, please explain your response?
12. Are there any other definitions that should be included?

Section G: Working with others

G1. The Cyber Security Centre for Jersey will play an active role in the cyber defence community, exercising its functions effectively and to be able to make arrangements, or enter into agreements, with other relevant stakeholders both locally and internationally, including other cyber emergency response teams.

G2. The Cyber Security Centre for Jersey will have the power to consult and co-operate, as it considers appropriate, with relevant law enforcement authorities. They may co-operate with any enforcement authority to enable the enforcement authorities to fulfil their obligations under the Law.

G3. The Cyber Security Centre for Jersey will participate in investigations carried out by other regulators and authorities if requested by that organisation. This would include

a. Jersey Competition Regulatory Authority;
b. the Jersey Office of the Information Commissioner;
c. Jersey Financial Services Commission;
d. States of Jersey Police; and
e. other local authorities or bodies, other internationally recognised cyber emergency response teams (CERTs) and reputable international bodies and allow them to engage with The Cyber Security Centre for Jersey in this way.

G4. The Cyber Security Centre for Jersey will not have any enforcement powers or any regulatory powers. This provision is merely to enable The Cyber Security Centre for Jersey to participate and offer advice if it is requested by the authority.

Section G: Working with others

13. Do you have any concerns regarding the ability of The Cyber Security Centre for Jersey to work with other key stakeholders, please explain your response?

Section H: Designation as a Single Point of Contact (SPOC)

H1. The Cyber Security Centre for Jersey shall be designated as the single point of contact (SPOC) as regards the security of network and information systems for Jersey. The Cyber Security Centre for Jersey will have the power to liaise with the relevant authorities in any Member State of the EU and the wider network if considers it appropriate to help protect Jersey from cyber incidents, which by their very nature do not respect international geographical boundaries.

H2. The Cyber Security Centre for Jersey, as the SPOC for Jersey, to be required to submit a report at least annually to the Minister, to include the number of incident notifications received, the nature of the notified incident and the Operators of Essential Services impacted.

Section H: Designation as a Single Point of Contact (SPOC)

14. Do you have any concerns regarding the designation of The Cyber Security Centre for Jersey as the Single Point of Contact for Jersey with regards to the security of network and information systems for Jersey, please explain your response?
15. Are the reporting requirements of incident notifications received sufficient, please explain your response?

Section I: Mandatory reporting of a security compromise

I1. In line with many recognised global standards, mandatory reporting of cyber security incidents will be required for those organisations who are considered to be Operators of Essential Services (OES). The rationale behind this is that these services are considered essential to Jersey and by mandating reporting of cyber incidents will maintain the cyber security resilience of the island.

I2. As captured in the Definition in section F, the definition of an Operator of an Essential Service is:

> Operator of an Essential Service (OES) means a person or organisation who is deemed to provide an essential service for the Jurisdiction of Jersey. Identification of essential services are as follows:
>
> a. an entity providing a service essential for the maintenance of critical societal and/or economic activities;
>
> b. the provision of the service depends on network and information systems;
>
> c. and an incident would have significant disruptive effects on the provision of that service
>
> d. For example, these services for Jersey would include:

Table 2: Operators of Essential Services within Jersey

Sector	**Subsector**	**Provider of Service**
Energy	Electricity	Distributors of for Jersey, for example Jersey Electricity
	Oil	Distributors of for Jersey
	Gas	Distributors of for Jersey, for example Island Energy
Transport	Air and Water	Providers serving Jersey covering harbours, marinas, coast guard and airport, for example Ports of Jersey
Banking and Financial Service Providers		Those registered with Jersey Financial Services Commission (JFSC)
Health	Care providers	All public and private health care providers
Drinking water	Supplier and distributor of	Providers serving Jersey, for example Jersey Water
Waste Water		Government of Jersey
Digital Infrastructure	Telecoms providers	All telecoms providers serving Jersey
	Providers of Information and Network Services	Jersey infrastructure providers, web providers, .je domain registers

Public Administration	Parishes	All services offered by Parishes
	Island wide	Government of Jersey
Postal services		Providers serving Jersey for example Jersey Post
Food production, processing and distribution		Key retail and food service operators Major grocery providers of essential products
Jersey based Regulators		Regulators for Jersey, for example: Jersey Financial Services Commission (JFSC) Jersey Office of the Information Commissioner (JOIC) Jersey Competition Regulatory Authority (JCRA) Jersey Gambling Commission

I3. If an organisation is classed as an Operator of an Essential Service, it must inform The Cyber Security Centre for Jersey without undue delay and in any event no later than 48 hours of becoming aware of the cyber security incident, any security incident that has an effect on the operation of the service.

Reporting a Cyber Security Incident to The Cyber Security Centre for Jersey

I4. If an organisation falls into the definition of OES then they must report the cyber security incident to The Cyber Security Centre for Jersey. As a minimum the information to be reported to The Cyber Security Centre for Jersey within the first 48 hours of become aware of the cyber security incident must include the following:

a. the operator's name and the essential services it provides
b. the time the cyber security incident occurred
c. current status of the cyber security incident
d. the duration of the cyber security incident
e. information concerning the nature and impact of the cyber security incident
f. information concerning any, or any likely, cross-border impact of the cyber security incident; and
g. any other information that may be helpful to The Cyber Security Centre for Jersey

I5. For your information The Cyber Security Centre for Jersey shall issue detailed guidance on this prior to the mandatory reporting requirement coming into force.

Reporting a Cyber Security Incident to the users of a service

I6. Operators of Essential Services are also required to:

a. take such steps as are reasonably and proportionate for the purpose of bringing the relevant information, expressed in clear and plain language, to the attention of persons who use the services who may be adversely affected by the cyber security incident.

b. The relevant information required must include:

i. the nature of the cyber security incident;
ii. the measures that it may be reasonably practicable for persons who use the network or service to the take for the purposes of preventing the security compromise adversely affecting those persons;
iii. remedying or mitigating the adverse effect that the security compromise has on those persons; and
iv. the name and contact details of a person from whom further information may be obtained about the cyber security incident.

Reporting a potential Cyber Security Incident/Risk to the Cyber Security Centre for Jersey

I7. Operators of Essential Services are also required to inform The Cyber Security Centre for Jersey of any potential security incidents/risk that have the possibility to have effect on the operation of their services. The information provided as a minimum must include:

a. the operator's name and the essential services it provides;

b. information concerning the nature and impact of the potential cyber security incident;

c. information concerning any, or any likely, cross-border impact of the potential cyber security incident; and

d. any other information that may be helpful to The Cyber Security Centre for Jersey.

Section I: Mandatory Reporting

16. Is the mandatory requirement on Operators of Essential Services to report within 48 hours of becoming aware of a cyber incident to long a period of time, given the significant impact a cyber incident can have?
17. Do you believe any additional information should be reported to The Cyber Security Centre for Jersey, please explain your response?

Section J: The Cyber Security Centre for Jersey's legal obligations to protect information

J1. It is intention that The Cyber Security Centre for Jersey has a legal obligation to protect the information which it gathers and acquires in accordance with the risk posed by such data, and must have rules in place governing the security and confidentiality of information, including procedures for access to, and the handling, storage, dissemination and protection of, information.

J2. The Cyber Security Centre for Jersey must put in place appropriate measures taking into account available resources and its statutory duties to protect its facilities, information and information technology systems with the purpose of preventing access by those not authorised to do so.

J3. The majority of work that The Cyber Security Centre for Jersey will be doing is in relation to the national security of Jersey. With regards to protecting personal data Article 41 of the Data Protection (Jersey) Law 2018 provides that processing of personal data necessary for the purposes of safeguarding national security is exempt from data protection principles and the transparency and subject rights provisions of the Law. Therefore, The Cyber Security Centre for Jersey will be looking for exemption under this Article in order to carry out its stipulated duties and functions.

J4. It is important that organisations know they can freely share information with The Cyber Security Centre for Jersey. This means The Cyber Security Centre for Jersey needs to be exempt from Freedom of Information Requests in relation to national security. In order to achieve this The Cyber Security Centre for Jersey will have to have an exemption under Part 4 of the Freedom of Information (Jersey) Law 2011.

Section J: The Cyber Security Centre for Jersey's legal obligations to protect information.

18. Do you consider it appropriate that information shared with The Cyber Security Centre for Jersey should be exempt from the Data Protection Law on grounds of national security, please explain your reasoning?
19. Do you believe that information shared with The Cyber Security Centre for Jersey should be exempt from Freedom of Information requests, please explain your reasoning?

Section K: Fees and charges

K1. It is the policy intent that The Cyber Security Centre for Jersey be a grant funded organisation through the Government Plan. The grant should be sufficient to cover the services and functions as mandated.

K2. In addition to the grant, it is the policy intent that the Chief Executive Officer is able to raise funds through sponsorship (for example to support the running of key events like Cyber Security Awareness Month).

K3. It is also the policy intent that The Cyber Security Centre for Jersey to be able to levy fees and charges. Examples of when The Cyber Security Centre for Jersey might levy a fee or charge could be for shared procurement of a training course in incident response or shared delivery of annual incident response exercises. Or, if The Cyber Security Centre for Jersey agrees to share a resource with another body, or to provide shared services at some point in the future.

K4. The governance around fees and charges would be a matter of policy for the Board, in line with the specified objectives of the project.

Section K: Fees and Charges

20. Do you think it is appropriate for The Cyber Security Centre for Jersey to have the ability to levy fees and charges, please explain your reasoning?

Section L: Pan-Island cyber security resilience

L1. Discussions are ongoing with the States of Guernsey to explore the opportunities of working across the jurisdictions with regards to cyber security.

Section L: Pan-Island cyber security resilience

21. What benefits do you see of a joint Jersey-Guernsey cyber security centre?