



Jersey

CYBER SECURITY (JERSEY) LAW 2026

Official Consolidated Version

This is an official version of consolidated legislation compiled and issued under the authority of the Legislation (Jersey) Law 2021.

Showing the law from 1 September 2026 to Current



Jersey

CYBER SECURITY (JERSEY) LAW 2026

Contents

Article

PART 1	4
INTERPRETATION	4
1 Interpretation	4
PART 2	7
JERSEY CYBER SECURITY CENTRE	7
2 Administration of cyber security	7
3 Operational independence of Director	7
4 Technical Advisory Councils (TACs)	7
5 Advice provided by TAC	8
6 Codes of conduct	8
7 Powers of Minister in relation to JCSC	9
8 Accounts and annual report	9
9 Strategic plan	10
10 Annual assessment of funding by Minister	10
11 Independence of JCSC IT systems	11
PART 3	11
OBJECTIVES AND FUNCTIONS	11
12 Objectives of Director	11
13 Functions of JCSC: SPOC	12
14 Functions of JCSC: CSIRT	12
15 Functions of Director: general	13
16 Discharge of Director's functions by another person	13
17 Duty to issue guidance in relation to cyber security	14
18 Power to set or adopt cyber security standards	14
19 Power to assist in investigations	14
20 Power to provide cyber security services to States of Guernsey	15
21 Power to amend this Part by Regulations	15
PART 4	15
OPERATORS OF ESSENTIAL SERVICES	15

PART 5	15
SECURITY DUTIES ON OPERATORS OF ESSENTIAL SERVICES	15
PART 6	15
ENFORCEMENT	15
PART 7	16
INFORMATION SHARING AND CLOSING PROVISIONS	16
40 Information sharing	16
41 Power to amend this Law by Regulations	17
42 Transitional provisions.....	17
43 Consequential amendments	17
44 Citation and commencement	17
SCHEDULE 1	18
DIRECTOR OF JERSEY CYBER SECURITY CENTRE	18
1 Appointment and tenure of Director	18
2 Termination of appointment of Director	18
3 Disqualification for appointment, restrictions and exceptions.....	18
SCHEDULE 2	20
CONSTITUTION OF TAC	20
1 Application of Schedule 2	20
2 Constitution of TAC.....	20
3 Appointment of members	20
4 Disqualification for appointment	21
5 Code of conduct.....	21
6 Revocation of appointment.....	21
7 Remuneration of members	21
SCHEDULE 3	22
ESSENTIAL SERVICES, THRESHOLD REQUIREMENTS AND CONDITIONS	22
SCHEDULE 4	23
ENDNOTES	24
Table of Legislation History.....	24
Table of Endnote References	24



Jersey

CYBER SECURITY (JERSEY) LAW 2026

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

Commencement [[see endnotes](#)]

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 –

- (a) in relation to the JCSC, 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;
- (b) in relation to an OES, a 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 4.¹
- (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

[not in force]

PART 5

SECURITY DUTIES ON OPERATORS OF ESSENTIAL SERVICES

[not in force]

PART 6

ENFORCEMENT

[not in force]

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) ²
- (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 2026 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

[not in force]

SCHEDULE 4³

ENDNOTES

Table of Legislation History

Legislation	Year and No	Commencement	Projet No
Cyber Security (Jersey) Law 2026	L.22/2026	1 September 2026 – Parts 1, 2, 3 and 7 and Schedules 1, 2 and 4 (R&O.86/2026) Not in force – Parts 4, 5 and 6 and Schedule 3	P.107/2025
Cyber Security Law (Jersey) Amendment Order 2026	R&O.95/2026	1 September 2026	

Table of Endnote References

-
- ¹ Article 1(1) *amended by R&O.95/2026*
² Article 43(1) *spent, omitted*
³ Schedule 4 *spent, omitted*