Memorandum of Understanding

between Jersey Cyber Security Centre and the Jersey Competition Regulatory Authority and concerning cooperation and the sharing of information relating to cyber risks and incidents

Document No: JCRA 26/01

Date: 1 January 2026

Jersey Cyber Security Centre
1 Seaton Place
St. Helier
Jersey JE2 3QL
+44 (0)1534 500050
www.jcsc.je

Jersey Competition Regulatory Authority
2nd Floor Salisbury House, 1-9 Union Street
St Helier
Jersey JE2 3RF
+44 (0)1534 514990
www.jcra.je

1. Introduction

Jersey Cyber Security Centre

JCSC promotes and improves the Island's cyber resilience. JCSC is designed to act at arm's length from the Government of Jersey. JCSC supports critical national infrastructure, business communities, and citizens to prepare, defend and respond to cyber attacks in Jersey.

JCSC supports Jersey in several ways:

- acts as a Single Point of Contact for Jersey in relation to cyber security;
- monitors information on global cyber threats that may pose a risk to the Island;
- manages information security incidents;
- discovers and manages vulnerabilities;
- provides independent oversight of Jersey's overall cyber risk;
- shares knowledge to increase Jersey's cyber resilience; and
- protects Jersey's cyber security reputation by ensuring that JCSC meets the appropriate best practice standards for cyber security.

The Government of Jersey is proposing a new Cyber Security (Jersey) Law (***Cyber Law***). The Cyber Law will provide clear foundations for JCSC's operations and introduce new requirements on Operators of Essential Service (OES).

On 25 August 2023, by way of Ministerial Decision, the Minister for Economic Development, Tourism, Sport and Culture made a Ministerial Decision delegating certain functions. The Director (***Director***) of the JCSC (formerly CERT.JE) has the power to:

- enter into agreements in respect of JCSC and relating to cyber security in Jersey including but not limited to accepting tenders, placing and accepting orders, appointing consultants, agreeing and signing formal contracts and other forms of engagement;
- consult and co-operate, as he considers appropriate, with relevant authorities and bodies;
- monitor and analyse all available information, whether or not provided directly to JCSC, relating to internet and computer activity that may indicate a threat or risk which may affect Jersey, and take any action it considers necessary in response to those risks;
- analyse information received by JCSC relating to incidents affecting Jersey, and take any action he considers necessary to mitigate, or assist in the mitigation of, the effect of those incidents;
- identify vulnerabilities in network and information systems which may affect Jersey, and take any action he considers necessary to resolve those vulnerabilities and risks arising from them;
- understand current global cyber threats and how these may affect Jersey, and take any action he considers necessary in response to those threats;
- raise awareness in Jersey of cyber security risks and threats, and responses and mitigations;
- provide, and co-ordinate the delivery of, cyber security services;

- enable and promote the sharing of cyber security information in Jersey;
- increase the level of cyber resilience in Jersey to reduce the risk, and impact, of incidents;
- represent Jersey's cyber security interests within Jersey and internationally, including by participating in international co-operation networks including the network of cyber security incident response teams; and
- provide support to enable effective cyber security in Jersey.

The Jersey Competition Regulatory Authority

The Jersey Competition Regulatory Authority (the ***JCRA***) was established by the Competition Regulatory Authority (Jersey) Law 2001. Amongst other things, the JCRA has a duty under Part 5A, Article 24V of the Telecommunications (Jersey) Law 2002 (the ***Telecoms Law***) to:

> *'seek to ensure that providers of public electronic communications networks (**PECNs**) and public electronic communications services (**PECSs**) comply with the duties imposed on them under Articles 24K to 24N, 24S and 24T' (their **security duties**).*

These security duties relate to:

- identifying the risk of ***security compromises*** (as defined in the Appendix) occurring;
- reducing the risk of security compromises occurring; and
- preparing for the occurrence of security compromises.

'Security compromises' include the occurrence of a security event affecting the relevant network or service as a result of a ***cyber threat*** (as defined in the Appendix) (a ***Cyber Security Compromise***).

Purpose of this Memorandum of Understanding

This Memorandum of Understanding (***MoU***) has been entered into between JCSC and the JCRA because those parties envisage that there will be occasions where:

- the same risk or incident is reported to JCRA as a Cyber Security Compromise and to JCSC as a ***Cyber Incident*** (as so defined), requiring investigation or action by one or both parties;
- a risk or incident is reported only to the JCRA as a Cyber Security Compromise; or
- JCSC notifies the JCRA of an actual or potential Cyber Incident it has become aware of or has had reported to it

In any such event the parties may wish to share relevant information and the JCRA may wish to engage the JCSC to provide technical support in relation to an assessment or investigation.

In such circumstance the parties wish to establish by this MoU:

- the legal basis on which they will exchange information relating to the Cyber Security Compromise and/or Cyber Incident and what such information may comprise; and
- the operational basis on which such technical support would be provided (subject to the availability of suitable JCSC personnel).

The parties may supplement this MoU with standard operating procedures from time to time.

2. Operational basis for cooperation between JCSC and the JCRA

This MoU

The parties have entered into this MoU to summarise the approach agreed between the parties as to how they interact while carrying out functions under their respective legislation.

In respect of the Telecoms Law, it is expected that the parties may engage on the following topics and activities:

- the Telecoms Law and the JCRA's role in supporting and enhancing the security of Jersey, including the development of guidance, be it shared or individual, that has relevance to the Telecoms Law and those subject to it;
- in support of the JCRA's compliance monitoring function:
    - technical measures set out in any Codes of Practice;
    - support for Jersey's providers of PECNs and PECSs; and
    - development of any regulations or Codes of Practice under the Telecoms Law and related guidance
- in respect of potential or actual Cyber Security Compromises under the Telecoms Law:
    - assessing and addressing actual or potential risks to Jersey which may result in a Cyber Security Compromise;
    - assessing and addressing actual Cyber Security Compromises that have occurred impacting directly or indirectly on PECN and PECS provided in Jersey; and
    - development of any regulations under the Telecoms Law and related guidance;
- where the JCRA is considering or actively undertaking a formal investigation into a potential or actual Cyber Security Compromise; and
- engagement with other parties, including other regulators, on aspects of the Telecoms Law.

3. Sharing information

Introduction

The JCRA and JCSC may only provide information to the other if permitted, or not prevented, under applicable law. Subject to this, they will seek to share information that will enable or assist them to exercise their respective functions.

Both JCRA and JCSC will observe appropriate controls for the retention and sharing of information each may receive or gather in the course of performing its respective functions, extending to the instances where they may interact with each other.

Both parties have statutory gateways that enable sharing of confidential information gathered in the performance of their respective legal duties.

For the JCRA, this includes information gathered as part of the JCRA's compliance monitoring activities, in addition to any information received from PECN or PECS providers relating to a potential or actual Cyber Security Compromise (including but not limited to the identity of the PECN or PECS provider and of its personnel, details of any risk or incident and of the actions being taken and proposed to be taken by the PECN or PECS and technical details relating to the relevant network or services) comprising any document or information obtained in the exercise of its functions under Part 5A of the Telecoms Law.

For JCSC, the information which may be disclosed includes:

- information relating to the Cyber Incident or otherwise obtained in the carrying out of its functions, including JCSC assessments and findings; and
- technical information and expertise in the possession of JCSC.

Noting that legal gateways may allow for broad information sharing, both parties are mindful of the importance of keeping the confidential information that either may receive tightly controlled due to the potential impact upon those sharing it and the security of Jersey as a whole. In addition, the JCSC considers the trust placed in it as part of its role in supporting organisations in response to Cyber threats and incidents that may impact upon Jersey of paramount importance. For these reasons the parties agree to share such confidential information only where it is determined to be necessary to do so.

Principles of information sharing

The following sets out the principles of information sharing between the parties that are expected to be followed under the Telecoms Law in respect of the activities discussed previously:

- for the following purposes it is expected that no information of a confidential nature will normally be shared:
    - discussing the role of the Telecoms Law and JCRA in the security of Jersey generally; and
    - discussing the JCRA's compliance monitoring function and activities;

- where the parties may interact in respect of the JCRA's compliance monitoring regime, with a particular focus on a public telecommunications provider or providers and their compliance status, they agree to not to share information identifying a provider unless:
    - in the case of either party sharing information, the provider consents;
    - in the case of the JCRA sharing information with JCSC, without consent, where obtaining consent would unduly limit the JCRA in performing its functions effectively;
    - in the case of JCSC sharing information with the JCRA, without consent where the Director of the JCSC determines that it would be in the interests of the security of Jersey to do so; or
    - JCSC has the power to receive or share information under the proposed draft Cyber Security (Jersey) Law 202- as considered necessary.
- the same approach will apply where the parties may interact in respect of potential or actual Cyber Security Compromise;
- where the JCRA is considering or actively undertaking a formal investigation into a potential or actual Cyber Security Compromise or compliance failure it may share confidential information with JCSC. Where it is considered appropriate to do so the JCRA will seek to gain prior approval from the subject before sharing provider specific information.

This approach is reflected in JCRA's published Procedural Guidance and Guidance on Information Gathering and Enforcement, which together detail the Authority's approach to information sharing under Part 5A of the Telecoms Law.

The parties note that some information shared between them may be subject to restriction from sharing under the Data Protection Law or Freedom of Information Law, on the grounds of crime prevention or national security. The parties therefore agree, to the extent practicable, to consult with each other prior to sharing information with third parties.

Legal basis of information sharing

The parties note that the officers of the Minister for Sustainable Economic Development have assured them both that:

- the provisions of Article 24ZG(2) of Part 5A of the Telecoms Law will permit the disclosure of information by the JCRA to the JCSC; and
- disclosure of information under Article 24ZG(2) to the JCSC will in all circumstances be necessary in the interest of the security of Jersey.

The parties proceed on the basis that:

- while the JCSC remains part of the Minister's Department, it is permitted to disclose information to the JCRA; and
- the Cyber Law establishing the JCSC will contain provisions relating to information disclosure which permit the Director of JCSC to disclose information to the JCRA.

4. Other important provisions

Charging

There will be no charges levied from either organisation to the other through the course of their engagements. Engagement will be undertaken on a best endeavours basis as time and resources allow.

Dispute resolution

Any disputes arising from the interpretation or implementation of this MoU shall be addressed through senior-level discussions between the Chief Executives of the parties, with the aim of resolving the matter in a collaborative and timely manner.

Review and Amendment

This MoU will be reviewed on a regular basis and an updated version will be published on the websites of the JCSC and the JCRA when signed on behalf of each party.

Commencement and termination

This MoU will enter into effect when signed below by each party. This MoU may be signed by secure electronic means (such as Docusign).

This MoU shall remain in force unless terminated by either party on six months' written notice.

The parties will agree means for the secure exchange of notices.

Signatures

Signed for and on behalf of the Jersey Cyber Security Centre

Matt Palmer
_____
Matt Palmer, Director

Date: 19/12/25

Signed for and on behalf of the Jersey Competition Regulatory Authority

Stephanie Liston (Feb 4, 2026 14:41:15 GMT)
_____
Stephanie Liston, Chair

Date: Feb 4, 2026

Appendix

Definitions contained within this document

A ***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 nonrepudiation 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.

A ***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.

A ***security compromise***, in relation to a public electronic communications network or a public electronic communications service, means any of the following, unless otherwise authorised by law –

(a) anything that compromises the availability, performance or functionality of the network or service;

(b) any unauthorised access to, interference with, or exploitation of the network or service, or anything that enables such access, interference or exploitation;

(c) anything that compromises the confidentiality of signals conveyed by means of the network or service;

(d) anything that causes signals conveyed by means of the network or service to be –

(i) lost,

(ii) unintentionally altered, or

(iii) altered otherwise than by or with the permission of the provider of the network or service;

(e) anything that occurs in connection with the network or service and compromises the confidentiality of data stored by electronic means;

(f) anything that occurs in connection with the network or service and causes data stored by electronic means to be –

(i) lost,

(ii) unintentionally altered, or

(iii) altered otherwise than by or with the permission of the person holding the data;

(g) anything that occurs in connection with the network or service and causes a connected security compromise.

Signature: Matt Palmer (Dec 19, 2025 14:54:12 GMT)

Email: m.palmer@jcsc.je