
	CERT.JE – Service Description	Date	22/09/2023
	TLP: CLEAR Information may be distributed without restriction. Subject to copyright controls.	Page	1


RFC 2350 – CERT.JE

Version 1.7 - 22/09/2023

	CERT.JE – Service Description	Date	22/09/2023
	<div style="text-align: center; background-color: black; color: white; padding: 5px;">TLP: CLEAR</div> <p>Information may be distributed without restriction. Subject to copyright controls.</p>	Page	2

Contents

1.	Document Information.....	3
1.1.	About this Document	3
1.2.	Date of Last Update	3
1.3.	Distribution List for Notifications	3
1.4.	Locations where this Document May Be Found.....	3
1.5.	Authenticating this document.....	3
1.6.	Document identification	3
2.	Contact Information.....	3
2.1.	Name of the Team	3
2.2.	Address.....	3
2.3.	Time Zone	3
2.4.	Telephone Number	3
2.5.	Facsimile Number	3
2.6.	Other Telecommunication.....	4
2.7.	Electronic Mail Addresses.....	4
2.8.	Public Keys and Encryption Information.....	4
2.9.	Team Members	4
2.10.	Operating Hours	4
2.11.	Other Information	4
2.12.	Points of Customer Contact	4
3.	Charter	5
3.1.	Mission Statement	5
3.2.	Constituency.....	5
3.3.	Sponsorship and/or Affiliation	5
3.4.	Authority.....	5
4.	Policies	6
4.1.	Types of Incidents and Level of Support	6
4.2.	Co-operation, Interaction and Disclosure of Information.....	6
4.3.	Communication and Authentication	6
5.	Services.....	6
5.1.	Incident response.....	6
5.2.	Incident Triage.....	6
5.3.	Incident Coordination.....	6
5.4.	Incident Resolution	7
5.5.	Proactive Services	7
5.6.	Vulnerability Management.....	7
6.	Incident Reporting Forms.....	7
7.	Disclaimers.....	7
8.	Incident Classification Matrix	8

	CERT.JE – Service Description	Date	22/09/2023
	<div style="text-align: center; background-color: black; color: white; padding: 5px;">TLP: CLEAR</div> <p>Information may be distributed without restriction. Subject to copyright controls.</p>	Page	3

1. Document Information

1.1. About this Document

This document contains a description of CERT.JE in accordance with the Internet Society Request for Comment (RFC) 2350, "Expectations for Computer Security Incident Response". It provides basic information about CERT.JE, its channels of communication and its roles and responsibilities.

1.2. Date of Last Update

Version 1.6 April 2023.

1.3. Distribution List for Notifications

Changes are not currently notified.

1.4. Locations where this Document May Be Found

The current version of this document can be found at <https://cert.je/rfc2350.pdf>

1.5. Authenticating this document

This document has been digitally signed by the official CERT.JE PGP key.

1.6. Document identification

Title: RFC2350-V1.7
Version: 1.7
Document Date: 22nd September 2023
Expiration: This document is valid until superseded by a later version.

2. Contact Information

2.1. Name of the Team

Full name: Jersey Cyber Security Centre
Short name: CERT.JE

2.2. Address

CERT.JE
1 Seaton Place
St Helier
JERSEY
JE2 3QL

2.3. Time Zone


GMT / BST

2.4. Telephone Number

+44 (0) 1534 500 050

2.5. Facsimile Number

Not applicable

	CERT.JE – Service Description	Date	22/09/2023
	<div style="text-align: center; background-color: black; color: white; padding: 5px;">TLP: CLEAR</div> <p>Information may be distributed without restriction. Subject to copyright controls.</p>	Page	4

2.6. Other Telecommunication

Not applicable

2.7. Electronic Mail Addresses

Incident Reporting

For incident reporting, please contact us at incidentreports@cert.je

This email address is monitored by CERT.JE employees during office hours only.

Phishing email reporting

For notifications of phishing emails, please contact us at phishing@cert.je

This email address should be only used for phishing notifications where immediate support is not required.

General enquiries

For other matters such as administration related topics and general inquiries, please send us an email at hello@cert.je.

This email address should also be used for PGP signed /encrypted emails.

This email address is monitored by CERT.JE employees during office hours only.

2.8. Public Keys and Encryption Information

Our PGP fingerprint is shown below.

PGP Key ID: 7E2A 6E16 BCDA A13E

Type: RSA 4096

Fingerprint: 0AC5F1519E08E795920E423DDF144306CABC02E6

2.9. Team Members

The Director of CERT.JE is Matt Palmer. The team includes four other members of staff.

2.10. Operating Hours


The hours of operation are from 09:00 to 17:00 GMT/BST Monday to Friday, excluding Jersey public holidays. The team may operate out of these hours and days in the case of an emergency only.

2.11. Other Information

CERT.JE is in the process of applying for FIRST membership.

2.12. Points of Customer Contact

The preferred method for contacting us is via email. If it is not possible or advisable due to security reasons to use email, then the CERT.JE can be reached by telephone during business hours.

	CERT.JE – Service Description	Date	22/09/2023
	<div style="text-align: center; background-color: black; color: white; padding: 5px;">TLP: CLEAR</div> <p>Information may be distributed without restriction. Subject to copyright controls.</p>	Page	5

3. Charter

3.1. Mission Statement

The mission of CERT.JE is to *“prepare for, protect against, and respond to”* cyber-attacks on Jersey.

The vision of CERT.JE is *“for Jersey to be internationally recognised as a safe place to live and do business online”*.

CERT.JE operates according to the CERT.JE Code of Conduct.

3.2. Constituency

The constituency of CERT.JE is the jurisdiction of Jersey, including:

- a) all organisations established within the jurisdiction, including but not limited to the States of Jersey, public sector organisations, private and public 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
- 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 jurisdiction or its residents.

3.3. Sponsorship and/or Affiliation

CERT.JE is funded by the Government of Jersey. CERT.JE has TF-CSIRT Trusted Introducer listing and is working towards accredited status.

3.4. Authority

CERT.JE derives its authority from the States of Jersey via the Minister for Economic Development, Tourism, Sport and Culture. By virtue of the functions and powers vested in him under

- (i) Articles 26, 28(1)(b), 29A,30 and 30A of the States of Jersey Law 2005,
- (ii) Ministerial decision reference MD-C-2019-0092 and
- (iii) the States of Jersey (Transfer of Responsibilities and Functions)(Chief Minister to Economic Development, Tourism, Sport and Culture) Order 2019,

On 25th August 2023 the Minister delegated functions to the Director of the Jersey Cyber Security Centre (CERT.JE) as described in <https://statesassembly.gov.je/assemblyreports/2023/r.128-2023.pdf>.

	CERT.JE – Service Description	Date	22/09/2023
	<div style="text-align: center; background-color: black; color: white; padding: 5px;">TLP: CLEAR</div> <p>Information may be distributed without restriction. Subject to copyright controls.</p>	Page	6

CERT.JE is currently part of the Department for the Economy of the Government of Jersey. However, CERT.JE operates at arm’s length from the Government, regulators and law enforcement and it is intended that CERT.JE will become a separate legal entity in the future.

4. Policies

4.1. Types of Incidents and Level of Support

CERT.JE uses the incident classification matrix shown on page 9 to assess cyber security incidents. It should be noted that incidents can change in severity throughout their lifetime.

4.2. Co-operation, Interaction and Disclosure of Information

CERT.JE recognises the importance of operational cooperation and information sharing between CERTs, CSIRTs and other organisations which may contribute towards or make use of the services that CERT.JE provides.

4.3. Communication and Authentication

CERT.JE respects the sensitivity markings defined by the originators of information communicated to CERT.JE. CERT.JE protects all data including sensitive information in accordance with Jersey Law.

5. Services

CERT.JE provides services aligned to the FIRST CSIRT Framework¹ for our constituency.

5.1. Incident response

CERT.JE incident response services are available on an 8/5 (working hours) basis to our constituency and may be available outside these hours on an exception basis when approved by the Director or Head of Cyber Defence. All information and communication technologies related incidents are evaluated using a triage process. In-depth analysis is provided by technical experts when required.

5.2. Incident Triage

Assessment of the severity of the incident is made in line with the CERT.JE Incident Classification Matrix shown on page 8.

5.3. Incident Coordination

- Categorization of the incident and related information.
- Coordination and notification of other involved parties on a need-to-know basis, as per CERT.JE data sharing agreements.

¹ [CSIRT Services Framework Version 2.1 \(first.org\)](https://www.first.org)

	CERT.JE – Service Description	Date	22/09/2023
	<div style="background-color: black; color: white; text-align: center; padding: 5px;">TLP: CLEAR</div> <p>Information may be distributed without restriction. Subject to copyright controls.</p>	Page	7

5.4. Incident Resolution

- Potential analysis of compromised systems and/or networks as an incident responder of last resort for public bodies.
- Identification and remediation of the cause of a security incident (exploited vulnerability), and its effects.

5.5. Proactive Services

- Public outreach to constituents on cyber security matters such as new CVE's.
- CERT.JE monthly newsletter.
- Network monitoring to detect attacks as early as possible.
- Automated and manual threat information sharing with our constituency and other National CSIRTS / CERT's.
- Help, advice, and training for our constituents.
- Risk management support

5.6. Vulnerability Management

- Vulnerability discovery and research through passive and or active scanning.
- Handling of vulnerability reports communicated to CERT.JE
- Vulnerability analysis and reporting impact on constituency if required.

6. Incident Reporting Forms

Incidents can be reported via email at incidentreports@cert.je. CERT.JE requests that email notifications and or sensitive information be encrypted with our PGP public key.

When you report an incident, please provide the following information:

1. Contact details and organisation information
2. Summary of the incident/type of event.
3. The source and which system produced an alert
4. Affected systems (s)
5. Potential impact.

7. Disclaimers

CERT.JE assumes no responsibility for errors, omissions, or for damages resulting from the use of information contained within.



8. Incident Classification Matrix

Incident Category	Definition of Incident	Typical Victim Profile	Indicative impact
1*	A cyber event which causes sustained disruption to Jersey's Critical National Infrastructure, affects the economy or reputation of the island, or the wellbeing of islanders, and has the potential to impact the UK, Channel Islands, or other jurisdictions.	Critical National Infrastructure. Essential Services. Large number of organisations. Significant number of the Jersey community is impacted. Telecoms providers. Potential impact on UK CNI, services, large number of organisations or individuals internationally.	Public safety. Public Health. Loss of life. Significant or sustained disruption to public services. Severe economic consequences. Severe reputational impact. Realistic potential to extend to UK or internationally from Jersey
1	A cyber event which causes sustained disruption to Jersey's Critical National Infrastructure, affects the economy or reputation of the island, or the wellbeing of islanders.	Critical National Infrastructure. Essential Services. Large number of organisations. Telecoms providers. Significant number of the Jersey community is impacted.	Public safety. Public Health. Loss of life. Significant or sustained disruption to public services. Severe economic consequences. Severe reputational impact. Not expected to extend significantly beyond Jersey.
2	A cyber event which causes sustained disruption to an economic sector or impacts a significant proportion of individuals or organisations in Jersey.	Government of Jersey. Financial Services industry of Jersey. Significant number of public service or corporate organisations. More than one large organisation, their clients, customers, and supply chains.	Manageable disruption to public services. Significant economic and reputational consequences. Material impact on Government or a large number of commercial organisations plus their supply chains, clients, or customers.
3	A cyber event which causes sustained disruption to a significant organisation or group of organisations, their supply chain and client base, or a significant number of individuals.	A large organisation or a number of smaller organisations, their supply chain, clients, and customers. A significant number of individuals. Level 4 incidents impacting a vulnerable group.	Limited disruption to public services. Material loss experienced by a large organisation, their supply chain, clients, and customers. Welfare impact on vulnerable groups.
4	A cyber event which causes sustained disruption to multiple organisations or individuals in Jersey, or a larger organisation, their supply chain and client base.	Large organisations, medium sized organisations, or a group of individuals. Level 5 incidents impacting vulnerable adults or children.	Material loss to medium sized organisations, their supply chain, clients, and customers. Potential material loss to their supply chain, clients, and customers. Welfare impact on vulnerable individuals.
5	A cyber event which causes interruption to a small organisation or limited impact to a larger one, or impacts daily life for a member of the Jersey public.	A small organisation or individual(s), or limited impact on a larger group.	Some loss for a small organisation and potential loss to their supply chain, clients, and customers. Data theft or economic impact to a small group of individuals or an individual.