Jisc Cyber Security Incident Response Team (CSIRT)

RFC 2350

Version	1.02
Date	July 12, 2022
Review Date	11 May 2022
Approval	Steve Kennett
Author	David Batho

1.0 Document Information

This document contains information about the role of the Jisc CSIRT according to RFC2350. It provides basic information regarding the CSIRT, the ways it can be contacted and the services that it provides.

The RFC 2350 will provide relevant information on how to contact Jisc CSIRT and the key responsibilities of Jisc CSIRT services.

The Jisc CSIRT Mandate is available here.

1.1 Date of last update

10th May 2022

1.2 Distribution List for Notifications

Internal Jisc and accreditation and supporting bodies

1.3 Locations where this document may be found

Locations where this document can always be found are as follows: Jisc website (https://www.jisc.ac.uk/csirt) and Jisc Community (https://community.jisc.ac.uk/library/Jisc-services-documentation/about-csirt)

2. Contact information

2.1 Name of the Team

Jisc Cyber Security Incident Response Team (CSIRT), previously known as Janet CSIRT

2.2 Address

Jisc CSIRT
Jisc
Lumen House
Library Avenue,
Harwell Oxford,
OX11 0SG,
United Kingdom.

2.3 Time Zone

We are in the Universal Time Coordinated (UTC) time zone which is GMT+000 (+0100 during Daylight Saving Time).

2.4 Telephone Number

Telephone: 0300 999 2340

from outside UK: 00 44 1235 822 340

(Available Monday – Friday, from 0800 – 1800)

2.5 Electronic mail address

irt@jisc.ac.uk
It is recommended that sites whitelist this address.

2.6 Public keys and encryption information

Jisc CSIRT uses PGP to ensure the integrity, and when appropriate the privacy, of e-mail messages; and we encourage you to do the same when you contact us.

The public keys of the team and its individual members are available at public key servers worldwide.
Email Address: irt@jisc.ac.uk
Key Fingerprint: 1EED 6120 8725 8BFA 6627 C7FE EAAD 8BB2 5A0B 7ACE, accessible on international key servers.

2.7 Other information

Established 01st January 1993
This team has changed names:

- "JANET-CERT" from 1993
- "JANET-CSIRT" changed in 2007
- "Janet CSIRT" changed in 2015
- "Jisc CSIRT" from 2022

Jisc CSIRT facilitate   Jisc Cyber security community, which our members can share their challenges and issues in order to improve their security posture.

2.8 Points of customer contact

All email correspondence (including incident reports) should be sent to the mailbox at:

irt@jisc.ac.uk

Telephone: 0300 999 2340

From outside UK: 00 44 1235 822 340

3. Charter

3.1 Mission Statement

The mission of Jisc CSIRT is to be a professional, proactive, responsive, adaptable service; to educate our members and provide a leading world class incident response service to protect the UK education and research sector.

Jisc CSIRT will provide proactive incident management, coordination, training, and outreach to all our members and provide up to date advice and guidance to reduce threats and compromise of our members. To develop a culture of member first, to develop and nurture partnerships with all agencies, stakeholders, and partners.

We will ensure that we align with the Jisc's mission, to power and empower our members with technology and data they need to succeed.

Objectives

- Members First
- Develop and nurture partnerships with members, agencies, partners, and stakeholders.
- Investigate, analyse, and remediate incidents for our members and stakeholders.
- Embed nationally recognised standards and accreditations to improve quality and response.
- Ensure tools and technologies meet the needs of the organisation and assist in remediating security events.
- Collaborate with our members by recommending technologies, policies, and governance and provide training before and after a cyber incident.

3.2 Constituency

- Full contracted service to organisations connected to the Janet network (ASN786);
- Best efforts service to other organisations with an .ac[.]uk domain name.

Access to the Jisc CSIRT service is freely available to all Jisc-connected institutions.

Use of the service is subject to adherence to the:

Eligibility Policy

Acceptable Use Policy

Security policy

3.3 Sponsorship and/or affiliation

Parent Organisation - Jisc Technologies, Jisc

3.4 Authority

The main purpose of Jisc CSIRT in incident handling is the coordination of incident response. As such, we can only advise our constituency to act in accordance with the Jisc Security and Acceptable User policy and have no authority to demand certain actions outside of those policy agreements.

4. Policies

4.1 Types of incidents and level of support

Jisc CSIRT is authorised to address all types of computer security incidents which occur, or threaten to occur, in our constituency (see 3.2) and which require cross-organisational coordination. The level of support given by Jisc CSIRT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and our resources at the time. Special attention will be given to issues affecting constituent essential infrastructure and business continuity.

Jisc CSIRT will keep its constituency informed of potential vulnerabilities, and, where possible, will inform this community of such vulnerabilities before they are actively exploited.

4.2 Co-operation, interaction, and disclosure of information

Jisc CSIRT will cooperate with other organisations in the field of cyber security. This cooperation also includes and often requires the exchange of vital information regarding security incidents and vulnerabilities.

Jisc CSIRT operates under the restrictions imposed by UK law. This involves careful handling of personal data as needed by UK Data Protection law, but it is also possible that - according to UK Law – Jisc CSIRT may be forced to disclose information due to a law enforcement IPA notice.

Jisc CSIRT treats all submitted information as confidential by default and will only forward it to approved parties or stakeholders to resolve specific incidents when consent is implicit or expressly given.

4.3 Communication and authentication

For normal communication not holding sensitive information Jisc CSIRT will use conventional methods like e-mail. For secure communication PGP-encrypted or secure e-mail or telephone will be used.

If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust (e.g., Forum of Incident Response and Security Teams (FIRST), Trusted Introducer (TI),) or by other methods like call-back, mail-back or even face-to-face meeting if necessary.

5. Services

5.1 Incident Response

Jisc CSIRT will help constituent IT-security teams in handling the technical and organisational aspects of incident response. To support the incident response service being provided by Jisc CSIRT, the team will be following the four-step process outlined in in NIST SP 800-161.

Assistance or advice with respect to the following aspects of incident response management:

5.1.1. Incident triage

- Determining whether an incident is authentic

- Assessing and prioritising the incident

5.1.2. Incident coordination

- determine the involved organizations
- contact the involved organizations to investigate the incident and take the appropriate steps
- facilitate contact to other parties which can help resolve the incident
- send reports to other relevant CSIRT/CERTs
- Providing guidance on recovery

We mainly see ourselves as information hub which knows where to send the right incident reports to help and facilitate the clean-up of IT security incidents.

Jisc CSIRT will respond to incoming incident reports from humans within one hour during office hours Mon-Fri (08:00-18:00hrs UTC). During out of office hours (18:00hrs-00:00hrs UTC) incident response is dependent on issues being reported to us via telephone only.

If you have not received feedback to an incident report after two business days, we ask that you contact us again.

Auto-generated reports and data-feeds will be handled with the same service level agreement but without the need to give a formal response within office hours.

5.1.3. Incident resolution

- advise local security teams on proper actions to resolve incidents
- follow up on the progress of the concerned local security teams
- ask for reports
- report back

Jisc CSIRT will also collect statistics about incidents within its constituency. These will be used to inform the wider Security Operations Centre (SOC) and other Jisc directorates of Jisc CSIRT activities. Incident statistics are also available to constituent organisations, but only data that is related to that organisation.

5.2 Proactive activities

Jisc CSIRT endeavours to:

- raise security awareness in its constituency
- collect contact information of local security teams
- publish announcements concerning serious security threats
- observe current trends in technology
- distribute relevant knowledge to the constituency
- supply forums for community building and information exchange within the constituency

6. Incident reporting forms

Please contact the Jisc CSIRT via electronic mail or via the telephone number as stated in section 2.10

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications, and alerts, Jisc CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.