Cyber Incident Response

G-Cloud 15 Service Definition

1. Service Description

Organisations across the education and research sectors face an increasingly complex and fast-paced cyber threat landscape. Timely detection, expert guidance, and effective response to cyber incidents are now essential components of organisational resilience. As one of the UK's NCSC-Assured Cyber Incident Response (CIR) providers for the education and research community, Jisc delivers a comprehensive incident response service designed to help customers prepare for, withstand, and recover from cyber-attacks.

The Jisc Cyber Incident Response Service (CSIRT Enhanced) provides expert, assured support throughout the full incident lifecycle of Preparation, Identification, Containment, Eradication and Recovery, leveraging unique national-level capabilities to mitigate the impact of cyber incidents and strengthen long-term security posture.

Jisc operates Janet, the UK's National Research and Education Network (NREN). This infrastructure provides visibility and intelligence at a national scale, enabling Jisc to identify emerging threats and hostile activity targeting the sector. Through live network telemetry, primary threat intelligence feeds, and industry-leading analysis, the service delivers insights and containment options unavailable to traditional commercial providers.

This positions Jisc as the only NCSC-Assured CIR provider with:

- Access to nationwide education and research threat intelligence
- Enhanced network-level containment capabilities via the Janet Network
- Deep integration with sector-specific behaviours, infrastructure, and threat actors
- A long-established Cyber Incident Response Team trusted across UK academia

Together, these capabilities enable faster detection, more contextualised response actions, and more effective containment of active threats.

2. Service Eligibility Criteria

To utilise the Jisc Cyber Incident Response service (CSIRT Enhanced), the following eligibility criteria must be met, and must continue to be met during the term of the service:

- Janet Network Connection: Customers wishing to purchase Jisc's Cyber Incident Response service (CSIRT Enhanced) must have a Janet Network IP Connection.

3. Service Models

3.1 Retained Cyber Incident Response (CSIRT Enhanced)

The Jisc Retained Cyber Incident Response model is intended for customers who require assured and rapid access to incident response capabilities without delay at the point an incident occurs. A framework agreement is established in advance, enabling immediate call-off of services, agreed response service levels, and priority access to Jisc CSIRT expertise during an incident.

3.2 On-Demand Cyber Incident Response

The Jisc On-Demand Cyber Incident Response model is available to customers who have identified, or strongly suspect, that a cyber security incident has occurred or is ongoing and do not have an existing retainer in place.

This model provides the same scope of expert incident response, investigation, containment, and recovery support as the retained service; however, it is delivered without pre-agreed service levels, priority access, or the administrative efficiencies provided by a retained agreement.

4. Service Scope

4.1 Initial Incident Assessment

As part of its enhanced service offering, Jisc CSIRT provides a rapid and structured initial incident assessment to help organisations understand the nature and impact of an incident event. This includes quickly identifying any signs of compromise activity, evidence of attacker access, and the overall scope of the compromise. The team conducts a focused review of SIEM and EDR/XDR outputs, network telemetry, and other relevant log sources to build an accurate picture of the incident. Jisc CSIRT also draws on insights from its in-house Cyber Threat Intelligence (CTI) team to assess potential indicators of data exfiltration and to evaluate threat actor behaviour, enabling more informed and targeted response actions during the early stages of the incident.

4.2 Deployment of Endpoint Detection and Response (EDR)

As part of its service, Jisc CSIRT provides comprehensive support for the deployment of Endpoint Detection and Response (EDR) to strengthen containment, eradication, and recovery efforts, while reducing the risk of re-compromise. This includes deploying, or assisting with the rapid deployment of, Jisc-approved EDR tooling across affected or high-risk systems. The team validates EDR coverage to ensure effective visibility across all key endpoints and uses the tooling to identify signs of persistence, unauthorised accounts, lateral movement, and the presence of malicious tools. Jisc CSIRT also leverages EDR capabilities to support quarantine and isolation actions and to continuously monitor for reinfection attempts. The deployment of EDR forms a critical element of the overall technical containment strategy.

4.3 Containment Support

Jisc CSIRT provides comprehensive containment support to help limit attacker activity and stabilise the environment during an incident. This includes advising on and assisting with endpoint isolation through EDR, as well as coordinating credential resets and the enforcement of

multi-factor authentication to reduce the risk of further compromise. The team supports the removal of malicious tools, scripts, and persistence mechanisms, and guides organisations in improving account hygiene to restrict additional attacker movement. Where required, Jisc CSIRT also implements network isolation measures using Jisc's network-level containment capabilities to further protect affected systems and prevent ongoing intrusion.

4.4 Enhanced Network-Level Containment

Jisc CSIRT will utilise Jisc's network-level security capabilities provided as part of the Janet connection to enhance containment efforts:

- Support implementation of network-level blocks for C2 infrastructure, malware distribution channels and other malicious IPs.
- Leverage Jisc's network architecture to limit lateral movement or continued threat actor access.
- Apply emergency network controls (where feasible) to prevent reinfection or outgoing traffic linked to data exfiltration.
- Provide recommendations for segmentation and temporary access restrictions.

4.5 Digital Forensics & Incident Response (DFIR)

Where required and for major incidents only, specialist Digital Forensics and Incident Response (DFIR) support is provided to investigate and analyse cybersecurity incidents in depth. This includes forensic evidence collection and preservation, analysis of compromised systems, identification of attacker activity, timelines, indicators of compromise (IOCs), and associated tactics, techniques and procedures (TTPs). DFIR findings support incident scoping, regulatory or legal requirements, root cause analysis, and inform remediation and post-incident security hardening activities.

4.6 Recovery & Eradication Guidance

Jisc CSIRT provides structured recovery and eradication guidance to help organisations safely restore operations following an incident. This support includes advising on safe restore processes using known-clean backups and ensuring that appropriate validation is carried out before systems are reintroduced to the network. The team uses EDR and other tooling to assist with the eradication of attacker artefacts and confirms that systems are free from malicious activity. Jisc CSIRT also offers recommendations to prevent reinfection during the recovery phase, helping to ensure a stable and secure return to normal operations.

4.7 Post-Incident Security Handling

Following stabilisation, Jisc CSIRT will provide comprehensive hardening guidance including:

Active Directory Hardening

- Review of privileged accounts and administrative tiering.
- Identification of insecure configurations enabling lateral movement.
- Recommendations for identity hygiene, MFA enforcement, and privileged access restructuring.
- Guidance to align with the AD Tiering Model and Jisc/NCSC best practice.

Infrastructure & Endpoint Hardening

- Review patching posture, EDR coverage, and endpoint configuration.
- Network segmentation recommendations.
- Improvements to logging, monitoring and detection coverage.
- Ransomware Resilience Recommendations.
- Backup protection improvements.
- Credential handling hygiene.
- Long-term mitigation actions aligned to NCSC Cyber Assessment Framework.

4.8 Reporting and Documentation

Jisc CSIRT provides structured reporting and documentation throughout the engagement to ensure clear visibility of incident progress. This includes daily status update calls supported by a presentation outlining the current state of containment, known attacker activity, immediate risks, active work items, progress made, and the required next steps. At the conclusion of the engagement, Jisc CSIRT supplies a final incident report summarising the response activities and outcomes. This report is advisory in nature and is not intended to serve as a formal forensic report.

5. Service Management

5.1 Hours of Service

Jisc's Cyber Incident Response Service operates a split hour service:

- Full incident response, threat intelligence and digital forensics support via eyes on glass email ticket triaging and telephone support operate during core office hours (8am to 6pm).
- Emergency on-call via telephone support only operates outside of core office hours on a 24/7/365 basis.
- Where out-of-hours support is required, a multiplier of 1.5 shall be applied to the applicable day rate

5.2 Information Assurance

We are ISO27001 and Cyber Essentials certified, and use appropriate management infrastructure, network connectivity, staff security clearances and processes to deliver our security services in line with the Cabinet Office Security Policy Framework (SPF), NCSC guidelines (including, but not limited to, UK OFFICIAL) and the Data Protection Act (DPA) principles, all in line with GDPR. Our Cyber Incident Response Team (CSIRT) are NCSC Cyber Incident Response (CIR) Level 2 assured and CREST Accredited.

5.3 Service Pricing and Invoicing

Please refer to the Rate Card for day rates for this service.

6. Exclusions

The following are excluded from the service:

- Malware reverse engineering
- Legal advice
- System administration or engineering work beyond guidance

7. Customer Responsibilities

- Provide access to technical teams and systems.
- Deploy or assist deployment of EDR tooling as required.
- Implement recommended network and endpoint controls.
- Coordinate with third-party forensic provider.
- Maintain communication through a designated incident lead.

8. Jisc Responsibilities

- Provide qualified incident responders with sector-specific expertise.
- Use intelligence and tools available through the Janet connection.
- Act in accordance with NCSC best practice.
- Maintain confidentiality and handle data responsibly.
- Collaborate with the Customer, Jisc SOC (if subscribed), and third parties.

9. Assumptions

- Support will be provided remotely.
- Support will be required during business hours (Mon-Fri 8am to 6pm), where agreed additional out of hours support can be provided at an additional cost.

10. Acceptance Criteria

- Containment measures applied
- Recovery guidance delivered
- Hardening guidance provided
- Final report issued