## Security Policy

# Janet Security Policy

| | |
|---|---|
| Title: | Janet Security Policy |
| Reference: | MF-POL-007 |
| Issue: | 5.1 |
| Document owner: | Iain Brown, Chief Security Architect |
| Authorised by: | Henry Hughes, Chief Technology Officer (Security) |
| Date: | 2 March 2023 |
| Last reviewed: | 30 June 2025 |

## Document control

1. Superseded documents: MF-POL-007 issue 5, dated March 2022

2. Changes made: June 2025, change of owner and approver

3. Changes forecast: New owner to review and update - email help@jisc.ac.uk [1] with any suggestions for improvements.

## Summary

The Janet Security Policy describes the responsibilities of organisations connected to the Janet network and Jisc's responsibilities as owner and operator of the Janet network – the UK's national research and education network – to mitigate the risks that security incidents and misuse will damage the effectiveness of the Janet network and organisations connected to the network.

## Background

1. The Janet Network ("**Janet**") is the communications network operated by Jisc Services Ltd (Jisc) to serve UK education, research and other public sector purposes. Its primary purpose is to enable organisations in these communities to fulfil their missions of providing education, research, of supporting innovation, and of civic engagement more widely.

2. This Janet “**Security Policy**” covers two broad categories of organisation: those connecting directly to Janet in their own right (“**Connected Organisation**”); and those connecting indirectly, as a partner to the directly-connected organisation and with the connection made through the latter organisation’s own connection(s) to Janet (“**Partner Organisation**”). This Security Policy does not define the conditions under which such organisations are eligible to connect to Janet, and to use Janet services. The Janet Network Connection Policy does this.
3. The Security Policy is regularly reviewed and when required it is updated to reflect changes to the security landscape and advances in technology. The increase in damaging cyber security attacks in 2020 and 2021 within the education and research sectors has necessitated a further review of the policy, and following a consultation, additional principles have been incorporated to help best protect organisations connected to Janet. It is the policy of Jisc that, as a network for education and research, Janet will be most effective if it places as few technical restrictions as possible on the development or use of new applications and services, and security controls will only be implemented where there is a clear benefit. Therefore, the Janet Security Policy aims to balance security and operability to enable the UK to continue to be a world leader in education and research.
4. Jisc provides protective controls to defend the Janet network and the organisations connected to the network, and actively seeks to engage in threat intelligence sharing between all Connected Organisations, all government and law enforcement agencies involved in the protection of UK Education and Research, and in an international context, all equivalent National Research and Education Networks within appropriate legal frameworks.

# Documents referenced by the Security Policy

5. The following Janet documents are referenced by this policy and they can be found at **http://ji.sc/policies** [2].

*MF-POL-006 – Janet Acceptable Use Policy (Janet AUP)*

*MF-POL-053 - Janet Network Connection Policy*

*GEN-DOC-009 – Terms for Provision of the Janet Service (Janet Terms)*

# Scope

6. This policy applies to any organisation with a connection to the Janet network, whatever type of agreement covers the connection. In particular it covers Connected Organisations – those organisations that have a direct relationship with Jisc; and Partner Organisations - any eligible organisation that connects to a Connected Organisation as their partner (see **Note 1**).

# Operational and legal requirements

7. Being connected to any network – including the Janet network – brings associated risks that security incidents or misuse will seriously damage the effectiveness of the network itself (a summary of these risks can be found in Annex A), and that the impact of

incidents may rapidly spread far beyond the individual organisation, machine or user where they originate. These risks must be managed if the network is to fulfil its purpose, therefore, Jisc has adopted this Security Policy to protect the network and the organisations that use it.

8. The authority of Jisc as service provider, to protect the operation of the Janet network is established in the Janet Terms, under which, compliance with this Policy is a requirement for all organisations connected to the network. The Policy also places responsibilities on users of the network.
9. The overall goals of the Janet Security Policy are:

- To ensure that Connected Organisations have appropriate policies and technical controls in place to protect the Janet network, the networks connected to the Janet network and the computer systems and platforms using the Janet network from abuse.
- To ensure that mechanisms exist to aid the prevention and identification of abuse of the Janet network.
- To ensure an effective response to complaints and queries about real or perceived abuses of the Janet network.
- To ensure that the reputation of Jisc is protected and that the network can meet its legal and ethical responsibilities regarding its connectivity to the worldwide internet.

# The Policy

In this policy the word "**must**", or the term "**required**" mean that the requirement has to be met. The word "**should**" means that there may exist valid reasons in particular circumstances to ignore a particular requirement, but the full implications must be understood and carefully weighed before choosing a different course.

## Responsibilities

10. The Janet Terms place responsibilities on every person and organisation involved in the use or operation of the Janet network to protect the network against security incidents and breaches. In particular:

    10.1 It is the Connected Organisation's responsibility to ensure that they are compliant with all relevant UK and national legislation.
    10.2 Each Connected Organisation must ensure that all use of the Janet network by those individuals and Partner Organisations to whom it provides network access complies with this Security Policy and the Janet Acceptable Use Policy. The Connected Organisation must also ensure that information about security issues can be communicated rapidly within the organisation and to Jisc and that problems are resolved promptly.
    10.3 Each Connected Organisation and their Partner Organisations must ensure that its actions and those of the users for which it is responsible are safe for themselves and do not present a threat to others.
    10.4 Each user of the Janet network and the networks of Connected Organisations and their Partner Organisations must behave in accordance with this Security Policy and with any policies and procedures local to the Connected Organisation. The user must cooperate with their organisation and the network operators to

reduce security risks.
10.5 Jisc must ensure that the operation of the network is appropriately monitored, that the response to security problems is coordinated, and that temporary or permanent measures are implemented, up to and including disconnection, where necessary to protect the network or to comply with the law.
10.6 Connected Organisations are required to undertake an annual self-assessment security posture review to ensure awareness of strengths and weaknesses regarding security controls and culture. Completing this self-assessment will help Connected Organisations ensure their local security provision is best placed to benefit from the central services provided by Jisc as well as helping to secure the Janet network (see **Note 2**). Jisc reserves the right to request confirmation that a self-assessment has been undertaken.
10.7 Connected Organisations are strongly encouraged to ensure that any Partner Organisations to whom they provide network access complete a self-assessment security posture review as a condition of their connectivity.

# Points of Contact at the Connected Organisation

11. The successful prevention of security incidents and prompt resolution of those that do occur both depend critically on the rapid and accurate transfer of information between Connected Organisations and Jisc as operator of the network. Each Connected Organisation must provide Jisc with up-to-date details of one or more persons who will act as Security Contact(s) for the Connected Organisation. The Connected Organisation must ensure that its designated Security Contact(s) have appropriate knowledge, skills, resources and authority to fulfil their role. As a minimum, each Connected Organisation must provide the following information (see **Note 3**):

    11.1 Name, role; email address
    11.2 Distribution group, fan out or team email address
    11.3 Emergency phone number

12. Security Contact data must be reviewed and confirmed to Jisc on a quarterly basis (see **Note 3**).
13. The Security Contact(s) have roles in both the prevention and resolution of security incidents. Security Contacts must disseminate Jisc's warnings of general risks and precautions to appropriate people within the organisation(s) for which they are responsible, and to ensure that appropriate preventive measures are taken promptly. Security Contacts must ensure that any particular security breach or risk that has been reported to the Security Contact(s) by Jisc as affecting an organisation for which they are responsible is investigated and resolved promptly, and to inform Jisc that this has been done (see **Note 3**).
14. Security Contacts should notify Jisc of serious cyber security incidents even where no assistance is required as an incident may be part of a wider campaign and any information that can be provided may help other Connected Organisations (see **Note 3**).

# Responsible Action by the Connected Organisation and their Partner Organisations

15. Each Connected Organisation and their Partner Organisations must act responsibly to

protect the network. This includes:

15.1 Taking effective measures to ensure that there is no security threat to the Janet network or other Connected Organisations or their Partner Organisations from insecure devices connected to the Organisation's network (see **Note 4**).
15.2 Taking effective measures to protect against security breaches, in particular ensuring that recommended security measures are implemented.
15.3 Taking effective measures to ensure that security breaches can be investigated and that other users of the network are protected from the consequences of breaches.
15.4 Assisting in the investigation and repair of any breach of security.
15.5 Promoting local policies in support of this Janet Security Policy and pay due regard to the Prevent Guidance for England, Scotland and Wales, backed by adequate disciplinary and other procedures for enforcement.
15.6 Implementing appropriate measures for giving, controlling and accounting for access to Janet, backed by regular assessments of the risks associated with the measures chosen.
15.7 Taking reasonable measures to encourage its users to act responsibly in compliance with this Policy and the Janet AUP, and ensuring that they are enabled to do so through systems, procedures and training that support good security practice.
15.8 Security Contacts must notify Jisc if undertaking penetration testing or scanning on the Janet Network from outside of the Janet Network at least 1 working day in advance (see **Note 3**).

16. Each Connected Organisation must**** notify Jisc of any significant incidents or attacks which:

    16.1 have the potential to disrupt the continued operation of the Connected Organisation; and/or
    16.2 carry a likelihood that other Connected Organisations may experience a similar attack, or that the incident could spread to those organisations; and/or
    16.3 could have a negative impact on the reputation of Jisc or the education and research sector; and/or
    16.4 carry the likelihood of Government or national media interest.

**** Unless Connected Organisations are instructed by their insurer or law enforcement to not notify Jisc, in which case they are strongly encouraged to explain to them the assistance Jisc CSIRT can provide, which could help to minimise impact and provide valuable information. The Connected Organisation should notify Jisc CSIRT as soon as they are able.

# Monitoring, Enforcement and Reporting by Jisc

17. The Janet Terms authorise Jisc, as the service provider responsible for the Janet network, to require Connected Organisations and their Partner Organisations to comply with this Policy, to monitor the network where it has reason to believe there has been a breach of the Policy or other threat, and to take such actions as are necessary to protect the operation of the network and the security of services provided to Connected Organisations and their Partner Organisations. In particular, Jisc is authorised to:

    17.1 monitor use of the network, while respecting privacy and complying with national law, either in response to information about a specific threat or generally because of the

perceived situation.
17.2 undertake proactive scans in response to critical vulnerability alerts or actionable threat intelligence to identify vulnerabilities in customer equipment that may present a serious threat to the security of the Janet network or services provided over it, and report these vulnerabilities to the relevant Security Contact(s) (see **Note 5**).
17.3 implement such technical measures as are required to protect the network or its customers against breaches of security or other incidents that may damage the network's service or reputation. These may be temporary or longer-term controls. Each control will undergo significant testing and monitoring to ensure they provide an appropriate balance of security and usability to best protect users (see **Note 6**).
17.4 require a Connected Organisation, through its nominated contact, to fulfil its responsibilities under any of the Jisc Policies.
17.5 where a Connected Organisation is unable or unwilling to co-operate, initiate the process for achieving an emergency disconnection.
17.6 where permitted or required by law, or to protect the Janet network, Connected Organisations or their Partner Organisations, assist relevant authorities in their investigations concerning the Janet network, including notifying authorities of relevant incidents and sharing threat intelligence and guidance with Connected Organisations, Users, NCSC and, where applicable, government departments, funders and agencies to support data protection (see **Note 7**).

# Explanatory notes

**Note 1:** A Connected Organisation is responsible both for their own users and devices, and also for ensuring that any Partner Organisation that they provide a connection to exercises their responsibilities.

**Note 2**: To improve cyber security, Connected Organisations are required to complete an annual internal self-assessment review of security posture. Connected Organisations can use whatever model or framework works best for that organisation e.g. CIS controls, Cyber Assessment Framework, Cyber Essentials, ISO27001, or using internal risk assessments. Organisations are invited to share information on which frameworks or tools they find helpful on the Jisc Cyber Security Community Group: **https://www.jisc.ac.uk/get-involved/cyber-security-community-group** [3]

**Note 3**: Security Contacts should contact Jisc CSIRT via the details at **https://www.jisc.ac.uk/csirt** [4]. Connected Organisations are also encouraged to share information about cyber security incidents with peers via the Cyber community group ( **https://www.jisc.ac.uk/get-involved/cyber-security-community-group** [3]).

**Note 4**: The security of networked devices may, for example, be managed by a combination of direct configuration and maintenance, technical controls such as firewalls or router access control lists, system monitoring or probing, and delegation to appropriately skilled others. Where an organisation allows a device it does not own or control to connect to the network it is strongly recommended that consent to these normal operational measures be obtained as a condition of connection.

**Note 5**: To provide the best protection for Connected Organisations, Jisc will undertake active scans in response to critical vulnerability alerts or actionable threat intelligence. Jisc will identify what looks to be the least intrusive way of looking for vulnerabilities, and where

possible, will look to establish a test system to verify that it just detects the vulnerability and should not cause an issue. Jisc will only run scans that have a high level of confidence of not causing serious impact to Connected Organisations or their Partner Organisations. Jisc will also be cognisant of the timing of scans, particularly avoiding the period of confirmation and clearing unless operationally essential. Jisc will always inform Connected Organisations of any detected vulnerabilities. The IP address ranges from which scanning activity will be undertaken can be found in the Jisc Cyber community Group: **https://www.jisc.ac.uk/get-involved/cyber-security-community-group** [3].

**Note 6:** One such control is restriction of certain high-risk protocols for traffic inbound to Janet. In March 2023 Jisc moved from an opt-in Foundation GeoIP service to being on by default unless Connected Organisations request to opt-out, as described at https://www.jisc.ac.uk/ddos-mitigation [5]. Connected Organisations will be given reasonable notice in advance of implementing such restrictions and will be able to see the current list of restricted ports and protocols on the Jisc Cyber Security Portal at **https://cybersecurity.jisc.ac.uk/** [6] or by emailing irt@jisc.ac.uk [7]. Security Contacts will be able to request an opt-out of restrictions for specific IP addresses.

**Note 7:** See https://www.jisc.ac.uk/guides/networking-computers-and-the-law/disclosure-of-information-to-law-enforcement [8] for more information.

# Annex A: Risks to Networks and Networked Systems

All computer networks are exposed to threats, both internally and from the other networks to which they connect. Hostile traffic, both random and directed, is now a constant feature of the Internet. The risks to the network, the computers and organisations connected to it, include:

- **Breaches of confidentiality.** Organisations hold and have access to large amounts of intellectual property, both their own and licensed from others: the value of such property may be greatly reduced if it is disclosed to others. Organisations also handle a great deal of personal information about individuals who may suffer if it is not kept confidential: consequences range from a loss of privacy to partial or complete theft of identity.
- **Loss of integrity.** Information held on computers can be destroyed or modified, and unauthorised changes may be undetectable. The integrity of computers themselves may be compromised if intruders are able to take control of them, thus casting doubt on the accuracy of any results. Repeated failures can result in users losing confidence in computer systems at their own or other organisations.
- **Failures of availability.** Networks and the computers connected to them may be temporarily disabled either deliberately or accidentally by large flows of network traffic or through the deployment of malware such as ransomware, making them unusable. Network and computer staff may be unavailable for support or development activities if they have to spend their time dealing with security incidents.
- **Damage to reputation.** The reputations of Jisc and the organisations and individuals connected to it may be seriously harmed by security incidents or inappropriate use of the network. Many intruders like to advertise their successes, others may attack third parties using computers connected to Janet and to which they have gained control. Organisations whose systems are used in these ways are likely to be held responsible.

The use of Janet to disseminate unwanted, offensive or illegal material is also likely to be seen as misuse of a publicly-funded resource.

- **Legal action.** National and international law is increasingly concerned with data networks and is placing a growing list of obligations on those who provide them. Individuals, organisations and network operators who, by action or inaction, fail to meet their legal obligations may be punished by the criminal law, have substantial financial damages awarded against them or be required to modify or cease their networking operations.

The openness of Janet and other connected networks may allow the impact of a security breach to spread far beyond an original insecure system or action. The same openness means that it will rarely be possible to protect organisations and users against the immediate consequences of their insecure actions: more often it will be necessary to respond promptly to security breaches by isolating the systems and organisations affected until the problem has been resolved. However, the more secure individual organisations are, the more secure the Janet network will be.

---



**Links**
[1] mailto:help@jisc.ac.uk
[2] http://ji.sc/policies
[3] https://www.jisc.ac.uk/get-involved/cyber-security-community-group
[4] https://www.jisc.ac.uk/csirt
[5] https://www.jisc.ac.uk/ddos-mitigation
[6] https://cybersecurity.jisc.ac.uk/
[7] mailto:irt@jisc.ac.uk
[8] https://www.jisc.ac.uk/guides/networking-computers-and-the-law/disclosure-of-information-to-law-enforcement