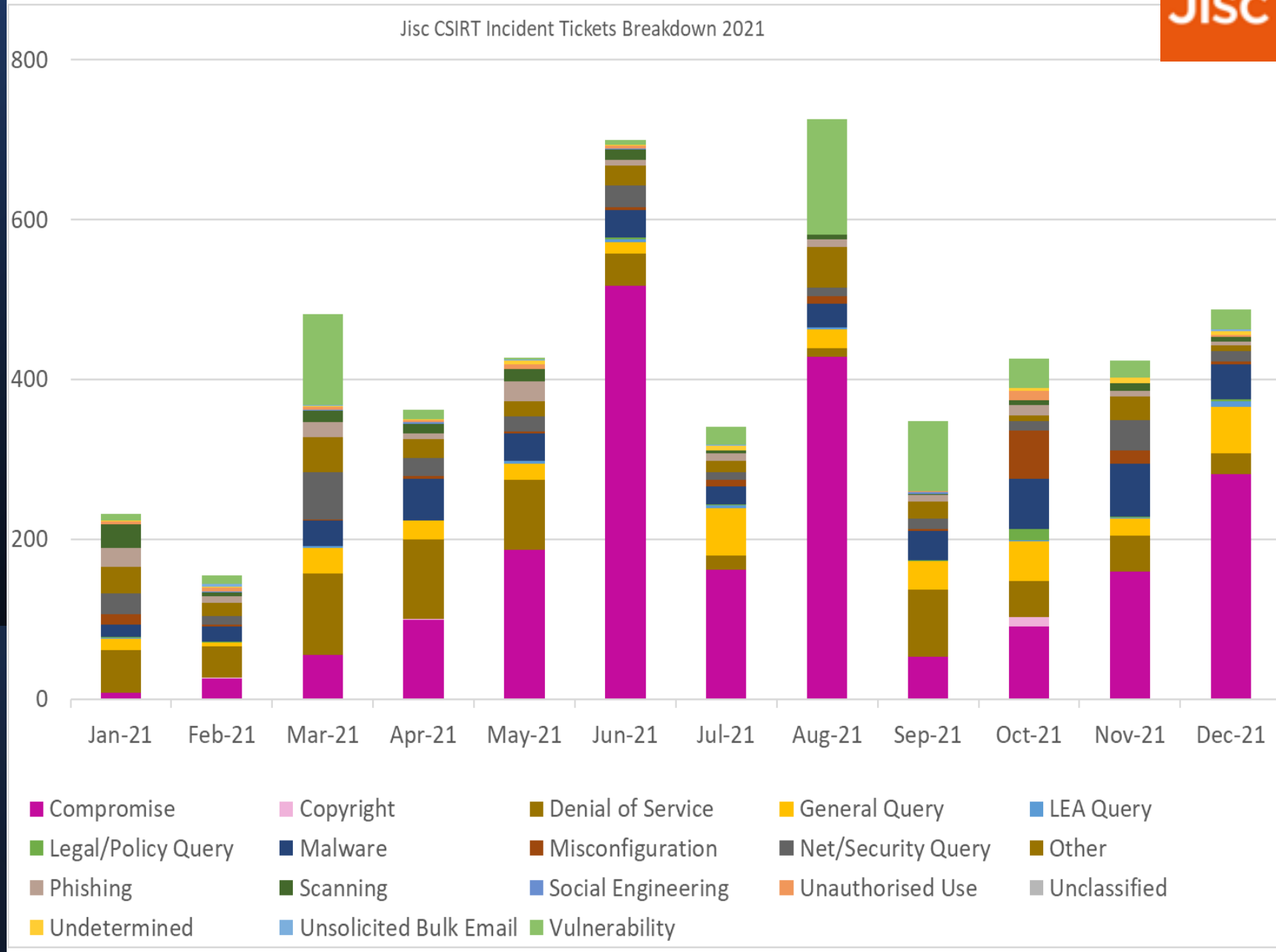
Making Janet more secure

John Chapman, Head of Janet policy and strategy

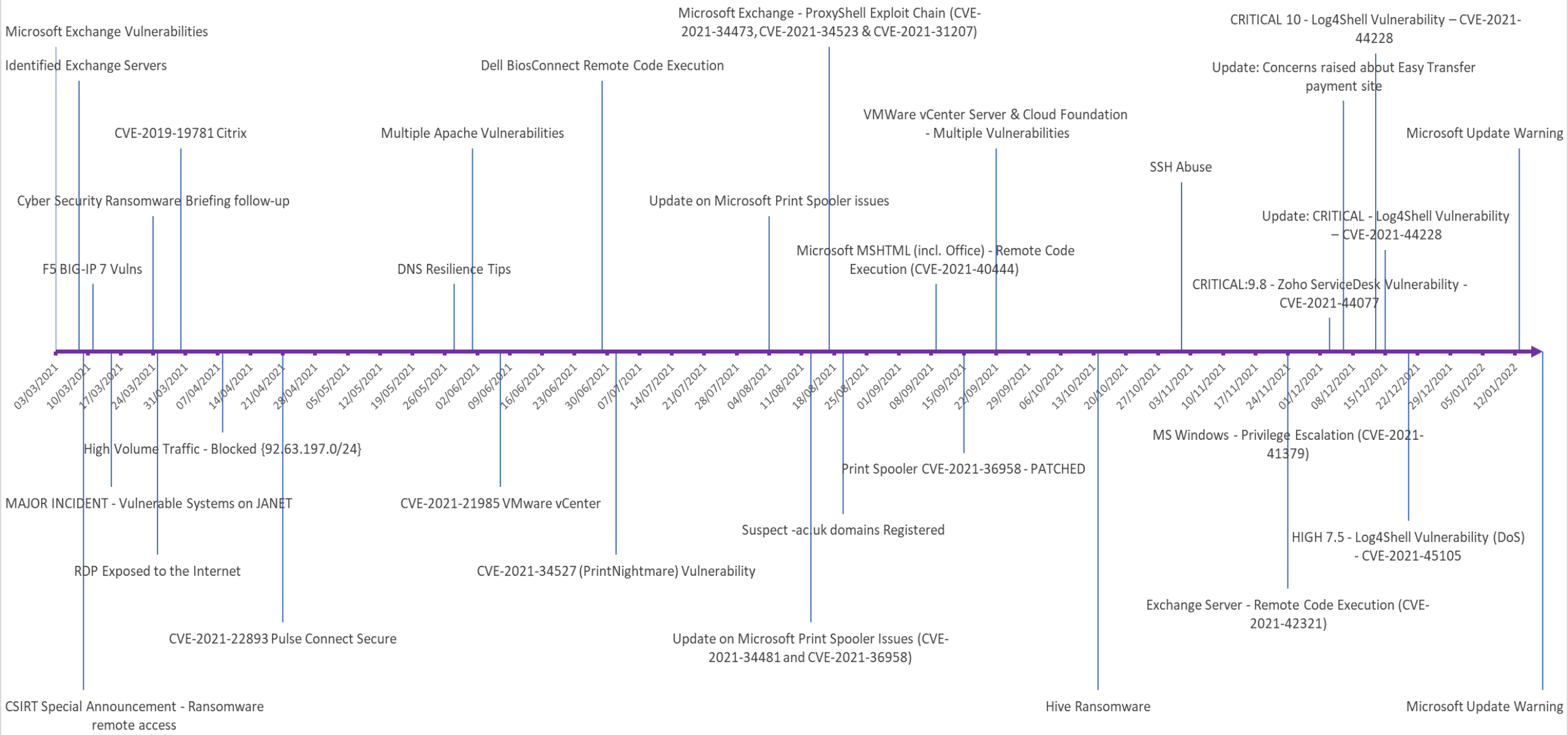
March 2022

Security Threat Landscape

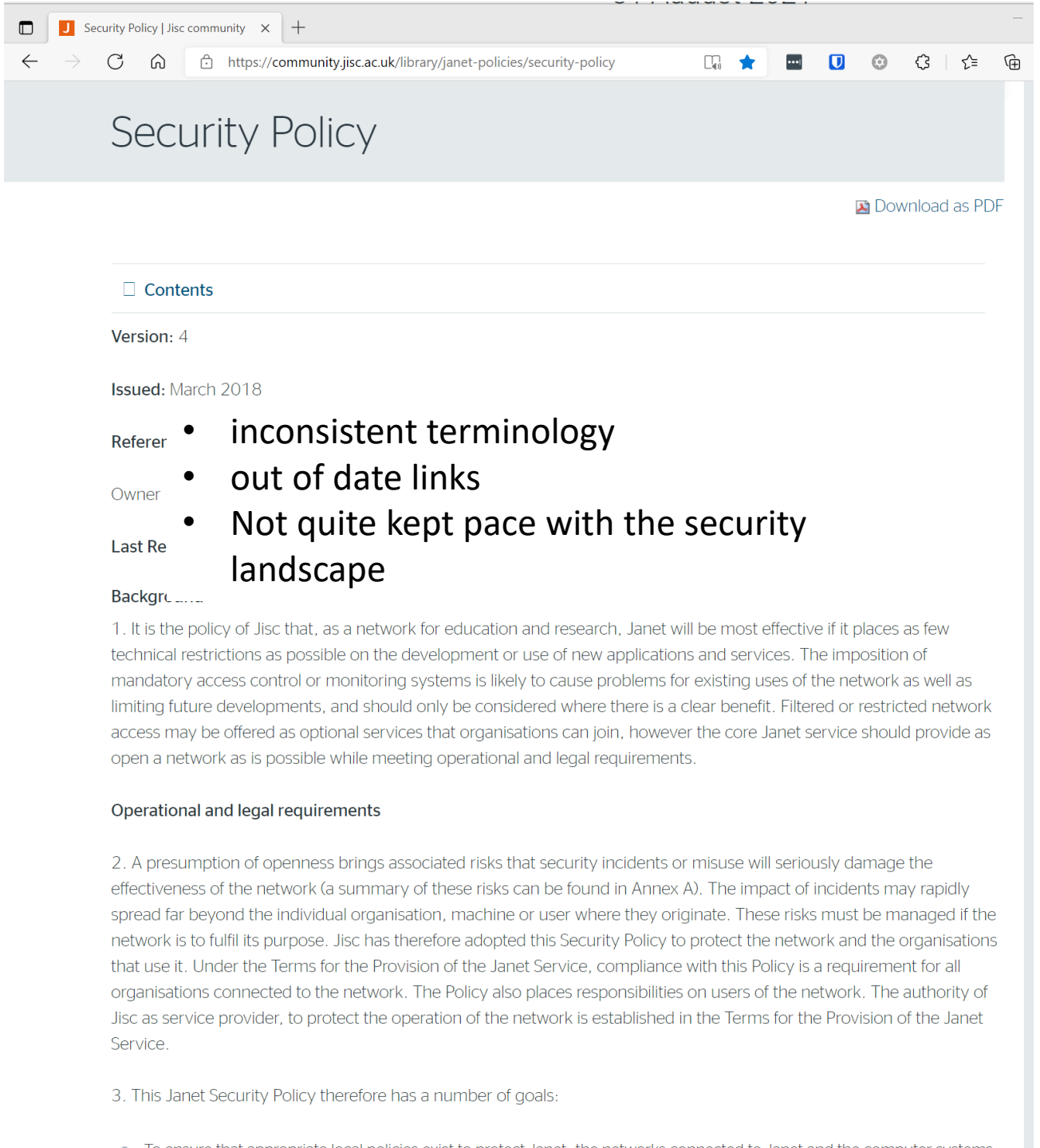
- Threat landscape continues to be challenging
- Concern that the sector continues to be targeted by a range of threat actors
- Jisc saw 15 ransomware attacks in 2020 and 18 in 2021
- Attacks are hugely disruptive
- Recovery is lengthy and expensive
- Impacts on cyber insurance: increased premiums, prerequisites for cover
- Necessitates defense in depth via proactive/preventative & reactive measures


Jisc CSIRT Incident Tickets Breakdown 2021
800
600
400
200
0
Jan-21
Feb-21
Mar-21
Apr-21
May-21
Jun-21
Jul-21
Aug-21
Sep-21
Oct-21
Nov-21
Dec-21
Compromise
Copyright
Denial of Service
General Query
LEA Query
Legal/Policy Query
Malware
Misconfiguration
Net/Security Query
Other
Phishing
Scanning
Social Engineering
Unauthorised Use
Unclassified
Undetermined
Unsolicited Bulk Email
Vulnerability

Vulnerability Notifications last 12 months



Janet Security Policy



- inconsistent terminology
- out of date links
- Not quite kept pace with the security landscape

Consultation 13/7-30/9 2021

Janet Security Policy Key Principles Consultation

Thank you for taking part in this consultation. This form consists of some explanatory text followed by 3 key principles we would like feedback on. Each principle has specific questions to help you frame your responses and it should take around 10/15 minutes to complete.

By providing information to this consultation you agree that you have asked us to process it as described in our standard privacy notice (https://www.jisc.ac.uk/website/privacy-notice). Any personally identifiable data will be kept for up to one year, and then deleted. You may instruct us to stop processing it at any time by contacting help@jisc.ac.uk with your request.

The consultation will be open until midnight on Thursday 30th September. Following the consultation, we will aim to publish a revised Janet Security Policy in Q4 2021.

For any questions related to this consultation, please email john.chapman@jisc.ac.uk

...

Purpose

The Janet Security Policy (https://community.jisc.ac.uk/library/janet-policies/security-policy) was first developed when the network and security landscape were very different to today. Although it has been updated from time to time, most recently in 2018 when Version 4 was published, these changes have been relatively minor.

With the huge increase in damaging attacks in recent years and months, the time is right to review the policy and to consult on additional principles that can help best protect Janet Connected Organisations, by balancing security and operability and enable the UK to be a world leader in education and research.

The aim of this consultation is to propose a new series of principles which, following the consultation, we will incorporate into a revised Janet Security Policy that will form part of the Janet Terms and Conditions.

The risks that security incidents or misuse will seriously damage the effectiveness of the Janet network must be managed if the network is to fulfil its purpose. Jisc provides protective controls to defend the Janet network and Janet Connected Organisations, and actively seeks to engage in threat intelligence sharing between all Janet 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.

As the service provider, Jisc acts to protect the operation of the Janet network. This is established in the Terms for the Provision of the Janet Service, and under these Terms, compliance with the Janet Security Policy is a requirement for all organisations connecting to the network. The Policy also places responsibilities on users of the network. The overall goals of the Janet Security Policy in supporting this remain unchanged. These are:

* To ensure that Janet connected organisations have appropriate policies in place to protect Janet, the networks connected to Janet and the computer systems and platforms using Janet from abuse (whether defined in the Janet Security Policy or other Janet Policies).

* 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.

New principle 1

GeoIP location blocking for certain high-risk protocols for traffic inbound to Janet

- Change existing function to opt-out rather than opt in (RDP port 3389)
- Ability to opt-out of any geoIP blocked ports/protocols at any time

New principle 2

Annual security posture review

- An internal self-review of your organisation’s security posture.
- Flexibility to choose how you do it
- No requirement to share the outcomes of your review with Jisc (but happy for you to do so)

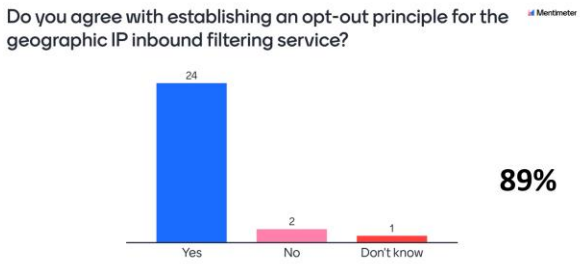
New principle 3

Proactive scanning

- Jisc will undertake regular active scans in response to critical vulnerability alerts or actionable threat intelligence.
- Jisc will always inform Janet Connected Organisations of any detected vulnerabilities.
- We will publish the IP address ranges from which scanning activity will be undertaken, to provide transparency of this activity.

1. Do you agree with establishing an opt-out principle for the geographic IP inbound filtering service?

More Details



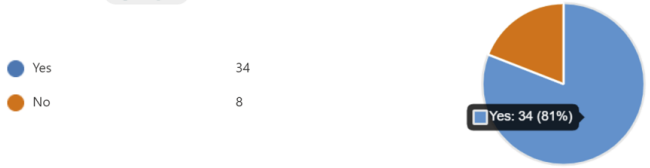
89%

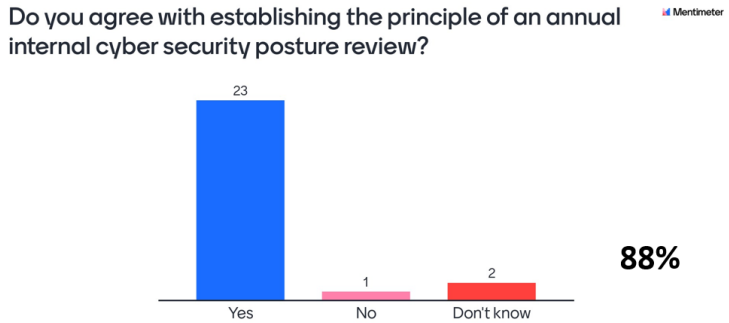
Responses received directly, via the consultation form, on CiSP, from UK-security, from the Jisc CISO Forum, via UCISA and from attendees at a Janet Tech2Tech briefing

Broad support for all three principles

3. Do you agree with establishing the principle of an annual internal cyber security posture review?

More Details Insights

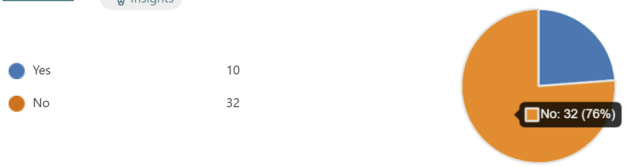


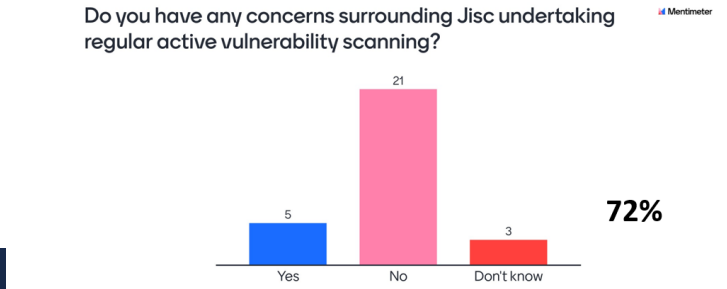


88%

9. Do you have any concerns surrounding Jisc undertaking regular active vulnerability scanning?

More Details Insights





72%

Janet Security Policy

Title:	Janet Security Policy
Reference:	MF-POL-007
Issue:	5
Document owner:	John Chapman, Head of Janet policy and strategy
Authorised by:	Jeremy Sharp, Janet CTO
Date:	3 March 2022 (Effective from 1 April 2022)
Last reviewed:	3 March 2022

Document control

1. Superseded documents: MF-POL-007 issue 4, dated March 2018
2. Changes made: Update to document. Harmonising of definitions across policies. Inclusion of 3 new principles following sector consultation in Summer 2021.
3. Changes forecast: None

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**.

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)**

* GEN-DOC-009 will be superseded in 2022 by the *Master Services Agreement for Janet Connection Services*

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
8. The authority of Jisc as service provider, to protec
with this Policy is a requirement for all organisatio
9. The overall goals of the Janet Security Policy are:

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.

- 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
nptly.
which it is responsible are safe

ehave in accordance with this
eir 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.

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

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**).

Note 3: Security Contacts should contact Jisc CSIRT via the details at **https://www.jisc.ac.uk/csirt**. 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**).

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.

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**.

Note 6: One such control is restriction of certain high-risk protocols for traffic inbound to Janet. During 2022 Jisc will move from the opt-in Foundation GeoIP service as described at **https://www.jisc.ac.uk/ddos-mitigation** to being on by default unless Connected Organisations request to opt-out. 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/**. Security Contacts will be able to request an opt-out of restrictions for specific IP addresses.

Janet Network Connection Policy

Title:	Janet Network Connection Policy
Reference:	MF-POL-053
Issue:	2
Document owner:	John Chapman, Head of Janet policy and strategy
Authorised by:	Jeremy Sharp, Janet CTO
Date:	3 March 2022
Last Reviewed:	3 March 2022

Document control

1. Superseded documents: MF-POL-053 issue 1, dated November 2019

2. Changes made: Update to document formatting and style. Clarifying the position of connecting Partner Organisations to support civic engagement

3. Changes forecast: None

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 "**Connection Policy**" defines the conditions under which all such organisations are eligible to connect to Janet, and to use Janet services. It 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**"). It also covers the granting of access to Janet to guests visiting an organisation with a Janet connection.
3. This Connection Policy does not address the question of any charges for services that may be levied by Jisc, as the provider of Janet. For further information on these, or advice on the interpretation of this policy, please contact the Jisc Service Desk by email on **help@jisc.ac.uk**.
4. The Connection Policy does not address the question of the use which may be made of Janet services once organisations are connected to Janet. The following documents referenced by this policy do this and they can be found at **ji.sc/policies**.

Categories of organisation connected to the Janet Network

12. In order to implement the principles, set out in *sections 6 - 11* above, any organisation proposing to connect to Janet, whether directly or as a Partner Organisation, is categorised as follows:

12.1 **Category 1**: Any organisation whose primary purpose is the delivery of state regulated education and/or state regulated research (whether publicly or privately funded); and where its regulation derives from one or more of the Jisc core funding bodies (see **Note 3**). This category includes, but is not

Note 4: Jisc has a long history of supporting Connected Organisations in their strategic management of relationships with commercial, public sector, cultural, social and civic organisations, in order to deliver services which benefit the economy and society. Previously known as business and community engagement, but now more commonly referred to as civic engagement, Jisc permits a Connected Organisation to share some of their Janet network connection bandwidth with an eligible Partner Organisation. This permission is subject to the terms described within this Connection Policy. The eligibility of a Partner Organisation to be connected in this way must be reviewed on an annual basis or when there is a change in the relationship between the Connected Organisation and the Partner Organisation to ensure the ongoing appropriateness of the agreement. If, upon review, the Partner Organisation is no longer eligible as set out in sections 12-13, then connection to the Partner Organisation must be terminated.

12.3 **Category 3**: Any other organisation, whatever its primary purpose, provided that its connection to and use of Janet is compatible with the principles and constraints set out in section 6 above. This includes, but is not limited to:

- schools, academies, museums, learned societies, charities and other organisations involved in education or research that do not by their regulatory status fall into Category 1;
- local, central and devolved government and their delivery partners utilising Janet in their delivery of public services and their other activities for the public good;
- health and social care organisations;
- Any organisation that a Connected Organisation requires to connect to support civic engagement (see **Note 4**).

13. Jisc itself, and any of its wholly or partially-owned subsidiaries, may also use Janet for the delivery of services to its membership and to others, and for any other mission or business purpose approved by its trustees.

Becoming a Connected Organisation

14. Permission to connect to and use Janet as a Connected Organisation is granted by Jisc and is in principle available to all categories of organisation as set out in *sections 12* and *13* above.
15. The process for connection will depend upon whether there is a grant-funded or other collective arrangement in place with Jisc for this purpose (as is the case for organisations in Category 1); or whether it is being provided on an individual, tariffed basis between Jisc and the organisation requesting a connection. This latter is normally the case for an organisation in either Category 2 or Category 3. The Jisc Service Desk can advise on the appropriate route. Please contact them via email at **help@jisc.ac.uk**, explaining in brief the rationale for eligibility of your organisation and the category in which your organisation sits.

Connecting a Partner Organisation to the Janet Network

16. When considering whether to grant a potential Partner Organisation access to Janet, the Connected Organisation should first conduct its own

Note 6: Potential use of the Connected Organisation's Janet bandwidth is of particular relevance for an organisation which receives its Janet connection via subscription to Jisc, rather than via a charge (tariff) that is proportional to the amount of bandwidth provided. A subscription entitles the Connected Organisation to as much Janet bandwidth as it reasonably needs to fulfil its mission, irrespective of subscription paid. Jisc is responsible for deciding this level of bandwidth, which it does by assessing both current consumption and likely future need. Jisc reserves the right to request details of their Partner Organisation(s) and for the Connected Organisation to disclose the proportion of its overall Janet usage that is accounted for by the activities of its Partner Organisation(s). Jisc needs to maintain fairness to all subscribers as to access to the extensive but ultimately finite bandwidth resources of Janet. If it concludes that use of a Connected Organisation's bandwidth by its Partner Organisation(s) is disproportionately high compared to other subscribers' behaviours, it may either decline to upgrade the Connected Organisation's bandwidth where it might otherwise do so; or it may levy a charge for the proportion of the bandwidth it determines is being used to support Partner Organisations. For this reason, a Connected Organisation should consider providing Janet access only to those Partner Organisations who have relatively modest bandwidth demands, as well as fitting the other criteria above. If a potential partner requires high-capacity access to the *Janet IP Connection Service*, it would be best served by an individual connection provided directly by Jisc.

Next steps

- Communicate opt-out processes for Janet threat defence *
- Investigate maturity models
- Supply chain security incident management
  - International recruiters
  - A UK HECVAT? (https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit)

http://ji.sc/policies

* Or whatever we decide the opt-out GeoIP functionality will be called…