Janet Policy Updates – FAQ

Janet Policy Updates – FAQ

A briefing on the changes to the Janet policies is available to watch at https://www.youtube.com/watch?v=lD1LBE3H-hg [1] with slides at https://cdn.eventsforce.net/files/ef-ot4nnkq56tkc/website/1340/making_janet_more_secure_tech2tech_march_2022.pdf [2]

The different Janet policies had slightly different terms for organisations connected to Janet. These have been harmonised as follows: “Connected Organisation” is an organisation connecting directly to Janet in their own right. In the previous Janet Security Policy this was called a “User Organisation”. “Partner Organisation” is an organisation 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.

References to Janet CSIRT have been updated to Jisc CSIRT and the contact email changed to irt@jisc.ac.uk [3]

Janet Security Policy

What are the main changes to the Janet Security Policy?

All the policies have been refreshed to update URLs and contact email addresses, formatted to look similar and terminology harmonised. The Janet Security Policy has also had three new principles included that are described below.

Principle 1: GeoIP location blocking for certain high-risk protocols for traffic inbound to Janet

Paragraph 17.3 explains that Jisc is authorised to:
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).

Note 6 explains:
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 [4] 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/ [5] . Security Contacts will be able to request an opt-out of restrictions for specific IP addresses.

What Ports and Protocols will you restrict?

For organisations that opt-in, we are currently restricting RDP traffic inbound to Janet on TCP port 3389 as exposing RDP publicly is a massive security risk and is a known threat vector used in ransomware attacks. The geoIP restriction is an additional layer of defence that may provide mitigation for RDP endpoints that are accidentally exposed, but should not be seen as a primary defence. Connected organisations should close all public RDP endpoints and move to either VPN, Azure AD Application Proxy or equivalent.

In the future, if other ports or protocols are identified as threat vectors and it is decided it is beneficial for them to be restricted on Janet then we will do so to protect connected organisations and the Janet network.

When will you start geoIP restrictions?

We can restrict inbound access to RDP traffic inbound to Janet on TCP port 3389 now for any connected organisations that want us to. To opt-in you can email Jisc CSIRT on irt@jisc.ac.uk [6] using the subject header 'Foundation Geo IP' providing the address space you would like filtered in contiguous IP address blocks.

Later this year we plan to move this geoIP filtering from opt-in to opt-out so it is on by default. Details on when this will happen and instructions of how to opt-out if you do not want this traffic restricted will be communicated at a later date.

Is that 3389 blocked from everywhere or just high-risk GeoIP locations?
The 3389 geo-blocking we have in place at the moment is to allow UK based source IP addresses through only.

What do you mean by "opting out of restrictions for specific IP addresses”?

Later this year when we to move this geoIP filtering from opt-in to opt-out so it is on by default organisations can decide to opt-out of this additional layer of defence. Instructions of how to opt-out if you do not want this traffic restricted will be communicated at a later date.

In the future, if other ports or protocols are identified as threat vectors and it is decided it is beneficial for them to be restricted on Janet then the same will apply: we will restrict inbound access to 'port X' unless an organisation decides to opt out. Organisations will be able to choose to opt-out at any time and will be able to opt-out of some or all of the restrictions.

Principle 2: Annual security posture review

Paragraph 10.6 explains that:
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.

Note 2 explains:
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 [7]

What do we have to assess ourselves against? Is there a pro forma?

Many organisations already undergo some sort of risk assessment or certification and given the variety of types of organisations connected to Janet we are being deliberately non-prescriptive as to how a self-assessment should be undertaken. The aim of this principle is to help organisations understand where their strengths and weaknesses are to help them become more mature. As everyone is starting from a different place we didn't want to exclude anyone. We know from feedback from some connected organisations that achieving Cyber Essentials is problematic, but we also know that some institutions are making good progress with ISO27001 or use CIS controls of CAF, for example. What we would like to do is to encourage organisations to share what they are doing and then we can see if there are frameworks or maturity models that are better suited to education and research organisations or to potentially look to co-design an education and research sector maturity model. Organisations are invited to share information on which frameworks or tools they find helpful in the Jisc Cyber Security Community Group: https://www.jisc.ac.uk/get-involved/cyber-security-community-group [7]

Do I need to share the result of my self-assessment with Jisc?

No. Jisc reserves the right to request confirmation that a self-assessment has been undertaken but there is no obligation on connected organisations to share the outcomes of reviews with Jisc. We would be very happy for you to do so, though, as understanding your strengths and weaknesses can help us to better protect your organisation and you may find it useful to compare with your peers.

When do we have to complete our posture assessment?

We aren't being prescriptive about this as we know a lot of organisations already do some form of risk assessment / posture check so this principle is about ensuring that all connected organisations do something to assess their strengths and weaknesses. It is up to you how and when you complete your assessment, but this should be at least once a year and would be good practice to complete when there are significant changes to your

environment or the security landscape.

Principle 3: Jisc CSIRT will perform more proactive scans to detect vulnerabilities in systems connected to the Janet Network.

Paragraph 17.2 explains that Jisc is authorised to:
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).

Note 5 explains:
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 [7].

How will you do the scans?

These vulnerability scans will typically be undertaken using masscan to find open ports that are affected and then using either an nmap script or a suitably scoped Nessus module.

How do we ensure this does not take place during change exception periods (Clearing and Confirmation) etc.?

As stated in Note 5, Jisc will be cognisant of the timing of scans, particularly avoiding the period of confirmation and clearing unless operationally essential. Unfortunately, when a new vulnerability is discovered, threat actors will be actively scanning for vulnerable systems connected to the internet so the quicker Jisc CSIRT can identify and inform affected organisations on the Janet network, the better.

Why are you now doing vulnerability scans?

Scanning for vulnerabilities is a key activity to help protect the network and connected organisations. The authorisation to undertake scans has been part of earlier versions of the Janet Security Policy, however the old wording suggested that this was done on an exceptional basis. Given the increase in serious attacks and the large number of vulnerabilities impacting connected organisations it was felt that the exception was becoming the rule so this principle is us being more open about how we are scanning and that we will be scanning more often due to the changes in the security landscape.

How do I know it is Jisc CSIRT scanning my systems and not a threat actor?

The IP address ranges from which scanning activity by Jisc CSIRT will be undertaken can

be found in the Jisc Cyber community Group: https://www.jisc.ac.uk/get-involved/cyber-security-community-group [7].

The policy says “14. Security Contacts should notify Jisc of serious cyber security incidents even where no assistance is required.” What if our insurance company tells us we can’t tell anyone about our incident?

Jisc recognises there may be some instances where legal or contractual obligations mean an organisation may be restricted in sharing information, which is why paragraph 14 is a “should” rather than a “must” requirement. Paragraph 16 provides more detail of when Jisc must be notified 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.

What other changes are there?

Clarification has been provided as to which statements are mandatory rather than recommended. 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.

Janet Network Connection Policy

What are the main changes to the Janet Network Connection Policy?

All the policies have been refreshed to update URLs and contact email addresses, formatted to look similar and terminology harmonised. The Janet Network Connection Policy has also had the position on connecting Partner Organisations to support civic engagement clarified, which can be seen in Note 4:

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.

To help ensure Jisc’s status as a private network and to maintain fairness to all subscribers, Note 6 provides clarity on our right to request details of Partner Organisations 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).

Although previously implicitly included within other bullets of 12.3, “health and social care organisations” are now explicitly listed as Category 3 organisations, as are “Any organisation

that a Connected Organisation requires to connect to support civic engagement".

Why are you using a URL shortener (ji.sc/policies)?

The ji.sc domain has been registered to Jisc since 2012 and is an established part of Jisc's brand to provide a more user-friendly way to deliver more memorable URLs. The Policy changes are important so finding an easy way to convey where they can be found in presentations and discussions is beneficial. Referring to http://ji.sc/policies [8] is more memorable than https://community.jisc.ac.uk/library/janet-policies [9]

Links
[1] https://www.youtube.com/watch?v=lD1LBE3H-hg
[2] https://cdn.eventsforce.net/files/ef-ot4nnkq56tkc/website/1340/making_janet_more_secure_tech2tech_march_2022.pdf
[3] mailto:irt@jisc.ac.uk
[4] https://www.jisc.ac.uk/ddos-mitigation
[5] https://cybersecurity.jisc.ac.uk/
[6] mailto:irt@jisc.ac.uk?subject=Foundation%20Geo%20IP
[7] https://www.jisc.ac.uk/get-involved/cyber-security-community-group
[8] http://ji.sc/policies
[9] https://community.jisc.ac.uk/library/janet-policies