

Contacts at Janet-connected organisations

- Responsibilities

The Janet Service Desk should be advised of any changes to site contact names or addresses. Janet(UK) cannot ensure that important information about the network reaches each organisation if contact details are not kept up to date. For example, changes to the fault reporting information may not reach management and operational/technical contacts, or information about security threats might not be passed to the security contact.

The Janet Service Desk sends Janet customers a Contacts form to amend each year but ideally sites should provide details of changes as they occur. Customers may wish to consider using generic e-mail addresses for the roles, e.g. [technical@customer.ac.uk](#) [1].

Responsibilities of Janet Contacts

- Management Contact
- Technical Contact
- Computer Security Contact
- Out of Hours Contact

At least one named contact must be provided for the technical, management and security roles, even if the same person is covering each one. The following notes explain what is generally expected of each contact.

Management Contact

The management contact must be able to make decisions relating to, and have the authority to contract for, the Janet connection. This contact is also required to sign the declaration of compliance with the [Janet AUP](#) [2] and [Security Policy](#) [3] (the declaration letter). Janet(UK) usually passes this contact's details to RIPE, the Internet registry for Europe, as the 'owner' of the IP addresses that are being requested, because this is normally the person in overall charge of IP address assignment for the organisation. However, you can specify an alternative RIPE contact on the JCUR if this is not appropriate. The management contact will normally be added to the mailing list for Janet News and similar publications, and to e-mail lists for news and support items.

Technical Contact

The technical contact is usually responsible for day-to-day decision making on technical issues concerning the organisation's network and the Janet connection. The name of this contact will normally be passed to RIPE, unless you provide an alternative contact on the JCUR.

Computer Security Contact

The Janet Security Policy ^[3] requires organisations with Primary Connections to nominate one or more people to be the first point of contact in dealing with any security incident that affects the organisation. The nominated contact is expected to be someone with technical knowledge and also with management authority since they may be asked to disconnect a computer from the network as a matter of urgency. Since it may be necessary to speak to a security contact at short notice, organisations may wish to nominate more than one person. However, in these circumstances they are expected to share information about current incidents. Ideally, an out-of-hours telephone number should be provided for these contacts.

When a message relating to an incident is sent, it is important that the security contact acknowledges that it has been received and that the problem is being investigated. If Janet CSIRT does not hear from the security contact that progress is being made to contain and resolve the incident then they are likely to escalate the problem through management to protect the operation of the network. The security contact will also receive general security information from Janet CSIRT relating to the prevention of security incidents. The contact is expected to pass these to appropriate people within their organisation and ensure that appropriate preventive action is taken.

Security contacts are also responsible for the activities of any Sponsored and Proxy Connections hosted by their organisation, and need to ensure that they are able to communicate quickly with those sites in case of problems. Security contacts are added to the UK Security JISCmail list and the mailing list for Janet News. Names and phone numbers of security contacts may also be given to law enforcement agencies if their investigations involve a Janet site.

Out-of-hours Contact

Technical, operational or security problems may arise outside normal working hours. It is therefore essential that the out-of-hours contact is available and has sufficient authority to take the appropriate action when such problems occur, such as Janet CSIRT needing to make an organisation aware of a security threat. If it is not possible to contact an organisation when necessary then Janet(UK) will take whatever action is needed to protect the Janet network, even if this involves disrupting the service to an individual organisation.

Source URL: <https://community-stg.jisc.ac.uk/library/janet-services-documentation/contacts-janet-connected-organisations>

Links

[1] <mailto:technical@customer.ac.uk>

[2] <http://community.ja.net/library/acceptable-use-policy>

[3] <https://community.ja.net/library/janet-services-documentation/contacts-janet-connected-organisations>