The Janet security contact

In order to investigate security reports and disseminate information within the Janet community, each Janet connected organization is expected to provide Janet CSIRT with security contacts. The requirements and expectations of security contacts may not be obvious, this page provides an outline of them.

The security contact

Janet CSIRT expects the security contact for a Janet organisation to be a person with time, competence, authority and management support to reliably ensure that the organisation takes prompt and effective action in response to requests and information from Janet CSIRT. We also expect you to ensure that your organization, users, visitors and customers adhere to the Janet Acceptable Use Policy and Security Policy.

The size and structure of organizations varies hugely and we do not expect our security contact to have direct control over all respects of their organization or third parties, but we do expect you to handle these organizational issues and provide a local point of coordination.

We also expect you to notify us when the details of your security contact change. We cannot tell if you have had staffing or organizational changes. **See Maintenance of Contact Information later in this note.**

E-mail

Janet CSIRT will normally communicate with the security contact by e-mail, and Janet CSIRT expects you to read messages and act on them within a few hours.

For almost every e-mail sent to you, you can presume that we require at least an acknowledgment unless it has been explicitly stated otherwise. We will not have any great knowledge of your organization, working practices and network, and it is difficult for us to tell the difference between e-mails which are not acted on, and e-mails which are not acknowledged. We recognize that in some cases it will take a little longer to complete any action necessary, and that you will need to triage and prioritize tasks.

Mail messages which Janet CSIRT sends will have a ticket number, inserted automatically both in the Subject: and in the body of the message. Ticket references are of the form

Janet_CSIRT#nnnnnn, including a six-digit serial number. In the message Subject: the ticket reference is enclosed in square brackets: [Janet_CSIRT#nnnnnn].
Please make sure that everything within the square brackets is maintained in the Subject: of further correspondence about the same issue. Most e-mail programs the "*Reply*" action will do this for you by default.

If your organisation also uses a partly automated ticketing system you may want Janet CSIRT to include your own ticket reference along with our own, which we are normally able to do. Please try to ensure that your system does not send automated acknowledgments or updates that take no account of our ticket number or the rest of the Subject: of our messages.

We do not need you to include in your reply the whole of our report or question to you. Selective quoting is recommended.

Role addresses

The e-mail address for the security contact may be that of an existing role such as *support* or *helpdesk*, or of a new role created specially for the purpose such as *csirt-contact*. The benefits are that usually role accounts are available to more than one person and are likely to be read more promptly, and that when staff move any changes to e-mail forwarding are purely local so that Janet CSIRT can use the role address without alteration. A possible disadvantage is that where people share a role it is possible for each of them to believe that another one is dealing with a request from Janet CSIRT whereas actually nobody is. Suitable working practices, or ticketing systems, are not hard to devise, implement and document.

We strongly recommend that you chose your role based address carefully, ideally based on RFC2141 which recommends you use abuse@… or security@… . Alternatively use a role based address such as cert@… or csirt@… . We are happy to accept other role based addresses, but please be aware that any unexpected addresses may cause problems with automated reports sent by Janet CSIRT. Please contact us for more information.

Local fan-out lists

Another approach also acceptable to Janet CSIRT and with advantages similar to those of using a role account is to operate a small local mailing list. The list receives mail sent to some address such as *csirt-contacts* and delivers a copy to a number of people on the basis that at any time at least one of them will be able to deal with it promptly. Some organisations think it appropriate for the IT Manager or some similar person to be included in the list, so that they are aware of security news and particular events affecting their organisation and can direct staff effort to suit. The danger of diluting responsibility arises in the same way as it does for a shared role account.

E-mail filters

Most organizations and many individuals apply some filtering to incoming e-mail messages, to more easily survive the flood of UBE, viruses and other abuse in the current hostile environment. One filtering or rejection technique is to examine message contents for patterns thought to indicate abuse and to be absent from wanted messages.

Unfortunately, filtering sotware and rules can wrongly classify the reports that Janet CSIRT may need to send you:

- Sometimes we send copies or partial copies of e-mail abuse (typically UBE, Unsolicited Bulk E-mail or *spam*) about which we want you to take some action. The presence of the copy material in our message can trigger the same response as if it was sent in actual abuse.
- We often cryptographically sign our reports using OpenPGP, and occasionally encrypt the contents. Some content filters are not able to distinguish between the encrypted parts of the resulting messages and an unidentified virus, and may reject them.

There are three kinds of ways you may be able to configure your filtering software or service to let our reports through without loss or delay:

1. You can give us a role contact address to which filtering is not applied.
   You should probably already be doing this for the postmaster address required by RFC 2821 and related RFCs, and you might extend it to the security or abuse addresses described in RFC 2142 and let us use one of those; or you can set up a special role address for this purpose only.
   - RFC 2821 [1] Simple Mail Transfer Protocol
   - RFC 2142 [2] Mailbox Names for Common Services, Roles and Functions
2. You can whitelist our originating e-mail address irt@csirt.ja.net [3].
   This exposes you to abuse from any bulk mailer, virus or worm that falsely uses our address, as does happen from time to time. Normal care and good practice will still protect you from actual damage, so that this is solution is not unworkable.
3. You can whitelist the IP addresses of our mail servers:
   212.219.244.160 mail1.csirt.ja.net
   195.194.48.203 mail2.csirt.ja.net
   This is effective as the addresses are stable and the servers well-managed.

You MUST NOT send delivery failure notifications for anything your filters decide not to deliver; you have to assume that the originator address of a message which is UBE or contains a virus is forged. We will never know you didn't get our report.

Telephone

Janet CSIRT will telephone for:

- urgent contact in case of an emergency where it is important to get the cooperation of the Janet organisation very quickly;
- escalation where we have had no substantive response to e-mail requests or the e-mail contact address appears not to work;
- detailed technical discussion in specific situations where we feel it will be more effective than e-mail.

Just as for e-mail details, it is not essential that a technician or network manager routinely answers the contact number given. It is more important that it is an attended number and that anyone likely to answer it will understand who we need to speak to and is able to put us in touch promptly. A number in an office shared by several network staff who are unlikely to be away from the office all at the same time may well be suitable; a helpdesk number where staff are trained to recognise calls from Janet CSIRT and to route them to the right people within the organisation is another possibility available in some organisations.

The office number of a technician or network manager who spends much of her time in other parts of the site, or the organisation’s PABX operator or receptionist, do not usually work well for this purpose.

Direct Dial-In numbers are preferred; but a switchboard number and extension are acceptable. Our experience is that a switchboard number and name only are not always effective in a larger organization.

An out-of-hours number should also be provided, if available.

Named person

Despite the advantages of role contacts, it is often helpful to have the name of one or more of the real people involved. One workable form of data is the name of a person and their personal extension, Direct Dial or mobile phone number, along with an e-mail address which is expanded to deliver to several people.

It is important that you have enough named contacts so that someone is available in the case of illness or holiday.

Multiple contacts

It is strongly recommended that organisations have at least two named persons, with e-mail address and phone number recorded, and ideally, an out of hours number. Normally we will send e-mail messages to all the addresses we have.

Mailing lists

Janet CSIRT maintains two e-mail lists UK-Security-announce and UK-Security. Both are operated by JISCmail using LISTSERV technology. Janet CSIRT is the list ”owner” (in LISTSERV terminology), and the -request addresses for the lists each forward messages to us for action.

- JISCmail [4]

Neither list is strictly secret or private, but circulation is limited. We ask you not to make the contents publicly available; you might copy them to an internal Web site, but not to your external one.
Janet CSIRT will add addresses at an organisation to either list or to both lists if the security contact there approves of the addition.

To join either or both of the lists, send your request to
UK-Security-announce-request@jiscmail.ac.uk [5] or
UK-Security-request@jiscmail.ac.uk [6]
as appropriate, and it will be forwarded to Janet CSIRT for consideration. If you know who the security contact is for your organisation you should instead ask them to write to us, as it will eliminate the stage of asking for their approval.

Compulsory; UK-Security-announce

Janet CSIRT uses the UK-Security-announce list to distribute material which is intended for all Janet organisations, either because it is important for all and requires action, or because it is relevant to many organisations and only the organisations themselves will know who they are.

All e-mail addresses supplied as security contact information are added to this list. Only Janet CSIRT is authorised to send messages to the list; the addresses on it must be valid for delivery of mail but (at least for this purpose) they need not be configured so that mail can be sent from them.

Optional; UK-Security

The UK-Security list is available for discussion; list members can send messages from their addresses as they appear in the list for expansion and delivery to all the members. Note that this does not work if the e-mail address from which your mail appears to be sent is different from the one entered in the list, even though that may be your preferred address for delivery. Your organisation’s mail should be configured so that your sent mail matches your delivery address; but if it does not and you want to use the discussion facility, you must ensure that it is your sending address that appears in the list.

In practice Janet CSIRT sends some announcements to both the UK-Security list and the UK-Security-announce list, which together make a virtual list UK-Security-all. JISCmail has a “ *Superlist*“feature which ensures that an address on both lists then only receives one copy of a message sent.

Multiple copies of messages

JISCmail has, of course, no automatic way to suppress duplicate copies of a message sent to one or both lists if they are to different addresses.
For instance,

- you may ask us to use in UK-Security-announce a role address which is a local list, while some or all of the people it expands to are on UK-Security with their personal addresses;
- or you may choose to have two or more addresses in UK-Security so that you can use either of them to post to the list.

The *NOMAIL* feature of JISCmail allows you to suppress list messages to any of your addresses. From the JISCmail front page set a password for your address using the link *Register Password* and then use the link *Subscriber’s Corner*.

- JISCmail [4]

Please do not over-use this facility. In particular make sure that at least one address remains set to have messages sent and will deliver them so that someone reads them and takes action.

Up [7] | Previous [8] | Contents [9]

Out-of-office replies

You must ensure that you do not send automatic replies to list messages, for a combination of reasons. On occasions when Janet CSIRT is trying to disseminate information, to be informed that you are out of the office is not satisfactory. In discussion use, there is no justification for troubling Janet CSIRT (as list owners) or contributors to the list with such responses, let alone passing an out-of-office response back to the address of the list itself and so to all list members.

You may be able to filter list messages so that they are delivered to a folder in your absence (and for that matter even when you are in the office) and you can read or dispose of them in your own time; otherwise for the discussion list UK-Security you will have to suspend your list subscription for the time you are away. Janet CSIRT will **not** do that for you; you can use the *NOMAIL* feature of JISCmail (see *Multiple copies of messages*) [7].

For the announcement list you may still apply some filtering but you will need to make your own arrangements, perhaps with one or more colleagues, for someone to read and respond to any messages needing action.

Genuine error messages may arise if your organisation’s mail service is experiencing difficulty; these will always be delivered to Janet CSIRT and may convey useful information, and there is no need to try to suppress them. Such error reports come from your organisation’s mail server and not from your own desktop mail program.

For the information of anyone wishing to process or filter list messages automatically, lines such as these from the message header should be a positive identification.
For a message sent to both the UK-Security and the UK-Security-announce lists:

Sender: General security announcement from Janet CSIRT <UK-SECURITY-ALL@JISCMAIL.AC.UK [10]> To: UK-SECURITY-ALL@JISCMAIL.AC.UK [10] Precedence: list

For a message sent to the UK-Security-announce list alone: Sender: Janet CSIRT special announcements <UK-SECURITY-ANNOUNCE@JISCMAIL.AC.UK [11]> To: UK-SECURITY-ANNOUNCE@JISCMAIL.AC.UK [11] Precedence: list

Maintenance of contact information

The database of contact details is held by the Jisc Service Desk. To update your details or to check what is at present recorded, please contact them by e-mail (service@jisc.ac.uk [12]) or telephone (0300 300 2212).

Other contacts

JSD also have other contact information for your organisation in relation to your connection to Janet and to any billing, management or policy questions which arise. Janet CSIRT has sight of some of this information and will use it if other routes fail.

Personal data

Jisc Privacy Notice [13]

In addition to the provisions of that policy, Janet CSIRT will normally not reveal the identity of security or other contacts at Janet organisations to people from other Janet organisations or elsewhere without obtaining their permission. However, Janet CSIRT's purpose is to respond to security incidents and concerns, and when urgent action is required we may consider it expedient to pass contact details directly to other parties involved in the incident. In such cases we will point out that the personal data is only to be used to resolve the immediate matter in hand.

Note also that in many cases the same personal data is published by someone else (perhaps in the organisation's Web pages or one or more *whois* databases). Neither Jisc nor Janet CSIRT accept any responsibility for use of information obtained in such ways.

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/janet-security-contact

Links
[1] http://www.ietf.org/rfc/rfc2821.txt
[2] http://www.ietf.org/rfc/rfc2142.txt
[3] mailto:irt@csirt.ja.net
[4] http://www.jiscmail.ac.uk/
[5] mailto:UK-Security-announce-request@jiscmail.ac.uk
[6] mailto:UK-Security-request@jiscmail.ac.uk
[7] http://www.ja.net/services/csirt/contact/contact-you.html#mult
[8] http://www.ja.net/services/csirt/contact/contact-you.html#mailinglists
[9] http://www.ja.net/services/csirt/contact/contact-you.html#contents
[10] mailto:UK-SECURITY-ALL@JISCMAIL.AC.UK
[11] mailto:UK-SECURITY-ANNOUNCE@JISCMAIL.AC.UK
[12] mailto:service@jisc.ac.uk
[13] https://www.jisc.ac.uk/website/privacy-notice