JANET Roaming Policy

Introduction

JANET Roaming aims to foster collaboration between education and research organisations by facilitating roaming network access for members of organisations that join the initiative.

Allowing authenticated visitors to obtain access to JANET is to the mutual benefit of the whole education and research community, but participation is entirely voluntary. Organisations will only provide visitor facilities if the benefits to them outweigh any problems. The success of the initiative in making visitor access widely available therefore depends on cooperation and responsible behaviour from all participants to ensure that visited organisations are not overloaded, that the Service is not disrupted and that any problems that may arise are dealt with promptly and effectively.

Each organisation has its own Acceptable Use Policy for use of its network, to accommodate local technical or organisational concerns, and this may well result in different rules applying to the guest service provided by different organisations. Visiting users must appreciate that their network access is a privilege, not a right, and must do their best to abide by all policies that both home and visited organisations apply. To this end, visitors should normally check the policies for each organisation they visit either before or early in their use of its network (visited organisations are required to make their local policies easily accessible, for example through the JANET(UK) JANET Roaming web pages or their local login page). In any case this JANET Roaming Policy requires that visitors immediately cease any activity that they are informed breaches local policy.

This Policy outlines the minimum requirements placed upon users, their home organisations, visited organisations and the operators of the JANET Roaming Service to ensure that each of these can be relied upon to play their part in ensuring the Service works effectively and securely. This is essential if the mutual trust required for the JANET Roaming Service to function is to be maintained. **All users and providers of the Service are required to comply with the Policy** on penalty of being barred from the Service. Participating organisations must also ensure that their computing regulations enable individual members who breach this Policy to be subject to an appropriate internal disciplinary process *irrespective of their location at the time of the breach.*

The Policy

Users

- Are responsible to their organisations (and legally) for all use of their credentials and any activities undertaken with the authority of those credentials. In particular, users must not allow their own credentials, or network access authenticated by them, to be used by others. If credentials may have been compromised the user concerned must report this to their home organisation;
- Must abide by restrictions applied by the home organisation and by JANET, including Acceptable Use Policies, Computing Regulations and Disciplinary Codes.

Restrictions imposed by the visited organisations must also be respected. Where Regulations differ, the more restrictive applies;
- Must follow instructions provided by their home organisation to verify that they are connected to a genuine JANET Roaming Service that provides adequate security before entering their login credentials;
- Must act immediately on requests by authorised staff of visited or home organisation that relate to their use of the JANET Roaming Service.

Home Organisations

- Are responsible to the community for the good behaviour of users they authenticate;
- Must enforce this JANET Roaming Policy on users they authenticate and investigate security breaches affecting their accounts, if appropriate informing any visited organisations that may be affected;
- Must promptly disable, at least with respect to JANET Roaming, accounts of users who have left the organisation;
- Must make their users aware of roaming conditions, including Regulations and Acceptable Use Policies;
- Must educate their users to follow best security practices when using the Service, including how to identify a genuine JANET Roaming Service;
- Must provide support for their users when roaming elsewhere (as a minimum, web-based information should be provided);
- Must provide the JANET Roaming Service with up-to-date contact details and act promptly on reasonable requests from the JANET Roaming Service;
- Must inform JANET CSIRT promptly of any apparent breaches of security affecting the privacy of user credentials.

Visited Organisations

- Must ensure that systems that support visiting users are configured, maintained and operated securely, so as not to put the security of other organisations or their users at risk;
- Must make their own AUP readily available to roaming users;
- Must assist home organisations in supporting roaming users when required, though the home organisation must take primary responsibility;
- Must provide roaming users with sufficient information to identify the roaming services they provide (for example locations covered, JRS Tier(s) SSIDs and certificates used)
- Must keep sufficient logs to be able to trace Internet activity to an authenticated user, and keep these logs securely for a minimum of three months;
- If activity logs are collected (e.g. web proxy), must make the relevant portions available to home organisation and/or the JANET Roaming Service when these are required to investigate misuse;
- Must accept and log complaints of misuse and forward these promptly to the appropriate home organisation;
- Must provide the JANET Roaming Service with up-to-date contact details and act promptly on reasonable requests from the Service;
- Must inform JANET CSIRT of any apparent breaches of security affecting the privacy of user credentials.

The JANET Roaming Service

- Must protect security of participating organisations and systems by implementing best practice;
- May exceptionally reduce or remove service without notice when this appears necessary for operational or security reasons;
- Must record authentication attempts and outcome (if possible) and retain these records securely for a minimum of three months and a maximum of six months;
- Must provide relevant extracts of this record to home organisation or JANET CSIRT when requested to do so;
- Must inform JANET CSIRT promptly of any apparent breaches of security affecting the privacy of user credentials.

Technical Sanctions

As noted below, the design of the Service gives each party the ability to impose technical controls to protect themselves and the Service against those who represent an immediate threat. However, as the effectiveness of the Service relies on cooperation, such technical measures should be regarded as a temporary solution until the problem can be resolved. Possible technical controls include the following:

- The JANET Roaming Service may suspend an organisation's ability to participate in the Service, either as a home or visited organisation, for failure to uphold this Policy, as for the JANET Acceptable Use and Security Policies;

- Visited organisations may prevent use of their networks by all users from a particular home organisation by configuring their RADIUS proxy to reject that realm and their access points to re-authenticate users currently connected; in some cases a visited organisation may also be able to block a single visiting user, but this depends on the particular technology used. In both cases, visited organisations must inform JANET Roaming Technical support of such measures.

- Home organisations may withdraw an individual user's ability to use the Service by configuring their own RADIUS server.

If a technical sanction is imposed that affects other organisations this must be reported immediately to the JANET Roaming Service and JANET(UK) (as manager of the Service), who will endeavour to assist the organisations concerned to resolve the problem, allowing the full Service to be restored. If a technical sanction involves a particular home organisation then the visited organisation should inform that home organisation as a matter of courtesy.