Guidelines for system and network administrators

Contents

Introduction

System and network administrators, as part of their daily work, need to perform actions which, at times, may result in the disclosure of information held by other users in their files, or sent by users over the University's communications networks. This document sets out the actions of this kind which authorised administrators may expect to perform *on a routine basis*, and the responsibilities which they bear to protect information belonging to others. Administrators also perform other activities, such as disabling machines or their network connections that have no privacy implications; these are outside the scope of this document.

On occasion, you may need to take actions beyond those described in this document. Some of these situations are noted in this document itself. In all cases you must seek individual authorisation from the appropriate person for the specific action that you need to take. Such activities may well have legal implications for both the individual and the University, for example under the Regulation of Investigatory Powers, the Data Protection and the Human Rights Acts. You must therefore obtain such authorisation promptly in all circumstances, and records must be kept to help to protect you and the University from any charge of improper actions.

System and network administrators must always be aware that the privileges they are granted place them in a position of considerable trust. Any breach of that trust, by misusing privileges or failing to maintain a high professional standard, not only makes their suitability for their role doubtful, but could also be considered by the University as gross misconduct. Administrators must always work within the University's information security and data protection policies, and should seek at all time to follow professional codes of behaviour

Authorisation and authority

System and network administrators require formal authorisation from the 'owners' of any equipment they are responsible for. The law refers to "the person with a right to control the operation or the use of the system". In the University this person is the Registrar, who has delegated these rights to the Director of IT Services who is therefore usually the appropriate authority to grant authorisation to system and network administrators for *routine* activities. For non-routine activities, the Registrar has delegated these rights to the Head of Legal Services. You have both a right and a duty to be duly authorised by an appropriate person to undertake the activities set out in these guidelines.

If you are ever unsure about the authority you are working under you should stop and seek advice immediately as otherwise there is a risk that your actions may be in breach of the law.

Permitted activities

The activities covered by these guidelines can be classified as operational or policy. Operational activities are undertaken to ensure that networks, systems and services are available to users and that information is processed and transferred correctly, preserving its integrity. You are acting to protect the operation of the systems for which you are responsible. For example investigating a denial of service attack or a defaced web server is an operational activity as is the investigation of crime.

You may also play a part in monitoring compliance with policies which apply to the systems. These policies include those implicitly or explicitly set out in the University's Information Security Policy and the JANET Acceptable Use and Security Policies. In these cases the administrator is acting in support of policies, rather than protecting the operation of the system.

The law differentiates between operational and policy actions, for example in section 3(3) of the Regulation of Investigatory Powers Act, so the administrator should be clear, before undertaking any action, whether it is required as part of their operational or policy role. The two types of activity are dealt with separately in the following sections.

Operational activities

Where **necessary** to ensure the proper operation of networks or computer systems for which you are responsible, you may:

- Monitor and/or record traffic on those networks
- Examine any relevant files on those computers
- Rename any relevant files on those computers or change their access permissions (see Modification of data below)
- Create relevant new files on those computers

When undertaking any of these activities, you should act with due respect for users' reasonable expectations of privacy and adopt as light a touch as possible. Do not unnecessarily browse log files, for example, when you are looking for something specific.

Where the content of a file or communication appears to have been deliberately protected by the owner, for example by encrypting it, you must not attempt to make the content readable without explicit, specific authorisation from the authorised person or the owner of the file.

You must ensure that these activities do not result in the loss or destruction of information. If a change is made to user filestore then the affected user(s) must be informed of the change and the reason for it as soon as possible after the event.

Policy activities

Administrators must not act to monitor or enforce policy unless they are sure that all reasonable efforts have been made to inform users both that such monitoring will be carried out and the policies to which it will apply. If this has not been done through a general notice to all users then before a file is examined, or a network communication monitored, individual permission must be obtained from all the owner(s) of files or all the parties involved in a network communication.

Provided administrators are satisfied that either a general notice has been given or specific permission granted, they may act as follows to support or enforce policy on computers and networks for which they are responsible:

- Monitor and/or record traffic on those networks
- Examine any relevant files on those computers
- Rename any relevant files on those computers or change their access permissions or ownership (see Modification of data below)
- Create relevant new files on those computers

When undertaking any of these activities, you should act with due respect for users' reasonable expectations of privacy and adopt as light a touch as possible. Do not unnecessarily browse log files, for example, when you are looking for something specific.

Where the content of a file or communication appears to have been deliberately protected by the owner, for example by encrypting it, you must not attempt to make the content readable without explicit, specific authorisation from the authorised person or the owner of the file.

You must ensure that these activities do not result in the loss or destruction of information. If a change is made to user filestore then the affected user(s) must be informed of the change and the reason for it as soon as possible after the event.

Disclosure of information

You are required to respect the confidentiality of files and correspondence.

During the course of your activities, you are likely to become aware of information which is held by, or concerns, other users. Any information obtained must be treated as strictly confidential - it must neither be acted upon, nor disclosed to any other person unless this is required as part of a specific investigation. This means that:

- Information relating to the current investigation may be passed to managers or others involved in the investigation
- Information that does not relate to the current investigation must only be disclosed if it is thought to indicate an operational problem, or a breach of local policy or the law, and then only to management for them to decide whether further investigation is necessary

You must be aware of the need to protect the privacy of personal data and sensitive personal data (within the meaning of the Data Protection Act 1998) that is stored on your systems. Such data may become known to authorised administrators during the course of their investigations. Particularly where this affects sensitive personal data, any unexpected disclosure should be reported to the University's Data Protection Officer.

Modification of data

For both operational and policy reasons, it may be necessary for you to make changes to user files on computers for which you are responsible. Wherever possible this should be done in such a way that the information in the files is preserved:

- Rename or move files, if necessary, to a secure filestore, rather than deleting them
- Instead of editing a file, move it to a different location and create a new file in its place

- Remove information from public view by changing permissions (and if necessary ownership)

Where possible the permission of the owner of the file should be obtained before any change is made, but there may be urgent situations where this is not possible. In every case the user **must** be informed as soon as possible of any changes which have been made and the reasons for the changes.

You may not, without specific individual authorisation from the appropriate authority modify the contents of any file in such a way as to damage or destroy information.

Privacy policies

In a spirit of openness and transparency all services should have an associated privacy policy published. Each policy should be written in plain English and should be readily accessible to all users of the service. The policy should provide users with the following information:

- Details of all of the information collected as a result of them using the service
- The uses made of the information collected (the purposes of the collection)
- The retention period for the information collected
- Details of who will have access to the information collected
- The circumstances under which the information collected will be disclosed to others

IP addresses

As any IP address assigned to the University (or otherwise used within the University) can, in association with other data held by the University, be used to identify individual users, the University considers such IP addresses to represent personal data within the meaning of the Data Protection Act. As such, any processing involving University IP addresses must be carried out in accordance with the Act.

References

The JANET website has examples of how these guidelines would apply in a variety of situations.

It is not possible to list all the legislation which applies to the work of system and network administrators. However the following Acts are particularly relevant to the activities covered by this document. The University believes that if you follow these guidelines your activities will not be in breach of any of this legislation.

- The Regulation of Investigatory Powers Act (2000) and the secondary Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- The Data Protection Act (1998)
- The Human Rights Act (1998)

The Office of the Information Commissioner's Employment Practice Code (with supplementary guidance) includes a section on Monitoring at Work, including use of computers and networks.

Acknowledgements

The document A Suggested Charter for System and Network Administrators was adapted to reflect local arrangements, and permission granted by its author, Andrew Cormack, Chief Regulatory Advisor, JANET, is gratefully acknowledged.