

Corporate Information and Computing Services

Appendix 5: Charter for System and Network Administrators

Introduction

Members of staff across the University have responsibility for servers, multiple computer systems, or for part of the network for example as a departmental IT administrator, computer technician or web administrator. Such Authorised System and Network Administrators (henceforth referred to as Administrators) need to perform actions as part of their daily work which may result in awareness of information held by other users in their files, or sent by users over communication networks. This charter sets out the actions of this kind which 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, which have no privacy implications; these are outside the scope of this charter.

Authorisation and Authority

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". At the University of Sheffield, this authority will come from the Administrator's Head of Department, possibly via a Line Manager or Head of Research Group (henceforth referred to as Management).

Administrators may come across evidence of problems during normal operations or in the course of other investigations. Where this indicates an operational problem, the Administrator may choose to investigate or pass the information to others for investigation. However evidence of policy breaches that do not relate to a current investigation must only be passed to Management for them to decide whether an investigation is appropriate and what form this should take. Administrators must not abuse the power and trust given to them by Management and users. University staff have no special exemption from the law and investigation of certain types of offence, for example the viewing of child pornography, may put an Administrator at risk of breaching the law which could result in criminal prosecution.

If any Administrator is ever unsure about the authority they are working under they should stop and seek advice from Management immediately as otherwise there is a risk that their actions may be in breach of the law. Note also that CICS has overall responsibility of the operation of the network and over connections to the network as set out in University Regulations on the Use of Computing Facilities.

<http://www.shef.ac.uk/cics/guidelines/codeprac/compregs.html>

Permitted Activities

The duties of Administrators can be divided into two areas.

The first duty of an Administrator is to ensure that networks, systems and services are available to users and that information is processed and transferred correctly, preserving its integrity. Here the Administrator is acting to protect the operation of the systems for which

they are responsible. For example investigating a denial of service attack or a defaced web server is an operational activity.

Administrators may also play a part in monitoring compliance with policies which apply to the systems. For example the University may prohibit the sending or viewing of particular types of material; or may restrict access to certain external sites, or ban certain services from local systems or networks. The JANET Acceptable Use Policy prohibits certain uses of the network. In all of 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 they are responsible, Administrators may:

- monitor and record traffic on those networks or display it in an appropriate form;
- 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.

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

The Administrator 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 record traffic on those networks or display it in an appropriate form;
- 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.

Where the content of a file or communication appears to have been deliberately protected by the owner, for example by encrypting it, the Administrator must not attempt to make the

content readable without specific authorisation from Management or the owner of the file.

The Administrator 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

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

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

- Information relating to the current investigation may be passed to Management 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.

Administrators 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 their systems. Such data may become known to Administrators during the course of their investigations. Particularly where this affects sensitive personal data, any unexpected disclosure should be reported to the relevant data controller.

Modification of Data

For both operational and policy reasons, it may be necessary for Administrators to make changes to user files on computers for which they 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 off-line archive, 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 what change has been made and the reason for it.

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

Investigation of Incidents

On occasion, Administrators may be involved in the investigation of security breaches, complaints or other incidents. Under such circumstances, Administrators may be asked to take actions beyond those described in this charter. Some of these situations are noted in the charter itself. Such activities may well have legal implications for both the individual and the organisation, for example under the Human Rights Act.

In all cases the Administrator must seek individual authorisation from Management for the specific action they need to take. Departments need to define the level of staff empowered to authorise an investigation (the list for CICS appears in Annex 2). Departments need to

balance the serious consequences which can arise if powers are misused against the common need for timely action.

In dealing with a potential disciplinary case, Personnel Services or Students Services should be involved, as appropriate. Where there is the possibility of there being a serious breach of the law, the University Security Advisor should be approached before an investigation takes place. CICS can provide advice on handling such investigations and related matters such as the securing of evidence and the interpretation of log files.

Keeping good records, preferably against a pre-prepared checklist (Annex 1), will help to protect the Administrator and the institution from any charge of improper actions. When investigating complaints, the implication of any evidence should be carefully considered. For example it is quite simple for email addresses to be forged. It is possible that, though something was apparently done from a specific machine or account, the normal user was not the person involved. The records may not tell the full story and may not even be complete or accurate.

It is important to consider how best to handle an investigation and the proper role of the Administrator. For example in the case of an abusive email, the use of a computer is really incidental, and the matter would normally be best handled as a case of Harassment with the Administrator providing information as requested. However in the event of a security breach the investigation may need to be handled by an Administrator who would have a full understanding of the nature of the breach and the import of evidence collected.

Considerable technical efforts are put into security: firewall, passwords, controlled access to systems and monitoring for attempted intrusion. However in all this it is often human beings that are the weakest link. When discussing privileged information of any kind, the Administrator needs to ensure that the person requesting the information has the right to have it. This is particularly important in respect of dealings with outside organisations. Somebody purporting to be from say the Police particularly on the phone may not be, so the Administrator must always establish that they are not only dealing with who the person claims, but also that the Administrator is authorised to talk to them. Investigations must always be kept confidential to those who have the need to know.

References

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 charter.

- 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 Data Protection Act (1998);
- The Regulation of Investigatory Powers (RIP) Act 2000: Email and Telephone Monitoring
- The Office of the Information Commissioner publishes advice and guidelines from time to time, for example on Monitoring at work
- JISC have published Senior Management Briefing Papers which discuss the specific implications of legislation for the education community:

A selection of examples have been written to illustrate how the charter might be applied to particular situations.

Modifying or deleting information

Mail loops/quota problems

Two common situations cause problems for electronic mail systems: users who forward mail to themselves (thus creating a loop) and users who run out of quota on their inbox. In both cases the mailhub responsible is likely to be affected, potentially degrading the service to other users. This is therefore an operational problem. An Administrator is entitled to remove the offending configuration, or move mail out of the full mailbox. A copy of the moved information should be left available to the user, and the user informed as soon as possible.

Deleting messages from mailboxes

Administrators are sometimes asked to delete messages from mailboxes belonging to other users. This is almost invariably for policy reasons, and involves the destruction of information held by a third party. Such actions must be Authorised individually by Management.

Removing published information from a web server

Although this is a similar situation to the previous example, there is an additional legal complication. If material that is defamatory, breaches copyright, etc. is published on a web or other server, then the owner of the server may be held liable for the publication. For this reason any organisation with public servers is strongly recommended to have a formal procedure for preventing further distribution of such material if a complaint is received. This is commonly known as a 'take-down procedure'. As there are likely to be legal implications for the organisation, take-down procedures should not be left to Administrators to write. Administrators receiving complaints about defamatory or copyright material on servers should always bring these to the attention of the Management. File permissions can usually be changed to prevent further distribution without destroying the information.

Using logfiles

Investigating service failures

The job of a Administrator is to ensure that the system is available for Authorised users. Where faults or misuse threaten the availability of the service, for example if there is an unusual load or unexpected failures, then they are expected to investigate this. This is likely to involve examining relevant logfiles or network traffic. As the problems are concerned with the operation of the system, an Administrator may investigate without seeking specific permission, however any information discovered that is not relevant to the investigation must be treated as confidential.

Investigating receipt of inappropriate e-mail

If a local user complains about a particular e-mail they have received then there should be no problem in requesting their explicit permission for any inspection of their mailbox or files that may be necessary. Checks may also be needed on the logs of mail and other servers through which the message may have passed. If the mail has caused an operational problem then it should be dealt with as described above; if not then it will normally need to be dealt with as a policy matter. Before checking the logs of systems with multiple users, a warning should have been published that the logs may be examined for such purposes. Some e-mails may involve illegal content - these should be reported to the Management as soon as possible.

Using cache logs to trace fraud

A rather common request to operators of web caches and other proxies is to use their logs to trace illegal activity, for example the use of stolen credit card numbers to buy goods. Since such activities are criminal, there should be no difficulty about helping law enforcement

officers in their investigations. Note however that any personal data should only be released through the proper procedure as laid out in the Data Protection Act 1998. For criminal investigations the Police should provide a section 29(3) form as part of their request for information to satisfy the requirements of that section of the Act.

Using cache logs to monitor user activity

Cache logs can also be a fruitful source of information about user activity but, unless the activity is criminal or has caused an operational problem, such investigations must be treated as a policy matter. Users must therefore be informed in advance that such monitoring may take place. If the Administrator is not confident that this has been done they must not obtain or provide access to the information. Logs must only be used as part of specific investigations and not for general "fishing trips".

Monitoring use

E-mail monitoring

Some organisations wish to monitor the content of e-mail or other traffic in or out of their networks to check compliance with policies. Users should always be informed of the likelihood of such monitoring as a condition of use of the network. Policy monitoring that results in messages being seen by people other than the sender and recipient is illegal if users have not been informed, and Administrators should not be expected to participate in such monitoring unless they are sure that this has been done.

Screen/keyboard monitoring

Systems exist that can remotely monitor the screens and keystrokes of individual workstations. Such systems have the potential to be extremely intrusive and should be implemented, if at all, with extreme caution. One useful application is to allow the user to demonstrate a problem to a remote helpdesk; any such systems should always be under the user's control and it must be made clear before using them how to start and turn off the remote monitoring. Users must be informed of the possibility of such monitoring, and any information obtained must be treated as confidential.

Virus checking

Many organisations automatically scan e-mail messages for viruses. If this scanning is done by computers, and provided the process does not reveal the content of messages to Administrators or others, then there is no invasion of privacy and no obligation to notify users. However it is good practice to inform users of such systems, if only to forestall complaints when an infected message is detected.

Based on a document Copyright The JNT Association. All rights reserved.

Version

1.00

Annex 1

University of Sheffield, Computer Incident Record (version1, 2003)

Administrator's Name	Date
Brief description of the incident	
Printed name of Complainant	Signature of Complainant
Actions Authorised	
Printed name of Manager Authorising Action	Signature of Manager Authorising Action
Log of actions, detailing time, action, associated filenames etc.	
Signature of System Administrator	

Annex 2

Authorisation for Investigation in CICS

In the case of CICS, Authority for the Investigation of computer and network incidents comes from the Head of Department. The following have delegated authority:

- ⑩ the Deputy Directors
- ⑩ the Team Leader for Customer Services.

In the event of unavailability of any of the aforementioned, any pair of Team Leaders can authorise an investigation.