Charter for System and Network Administrators

This document is based on the draft prepared Andrew Cormack, Chief Regulatory Adviser at JANET(UK). That draft was approved by the Universities and Colleges Information Systems Association (UCISA). It has been amended for use at the University of Sussex.

Introduction

System and network administrators, as part of their daily work, need to perform actions which may result in the disclosure of information held by others in their files, or sent over communications networks where they are not the intended recipient. This charter sets out actions of this kind which authorised administrators may expect to perform *on a routine basis*, and the responsibilities which they bear to protect this information. 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 charter and are covered by the University's Information Security policy.

On occasion, administrators may need to take actions beyond those described in this charter. Some of these situations are noted in the charter itself. In all cases they must seek individual authorisation from the appropriate person in their organisation for the specific action they need to take. Such activities may well have legal implications for both the individual and the organisation, for example under the Data Protection and Human Rights Acts. Organisations should therefore ensure that they have information and procedures in place, including delegation of authority for routine requests, to ensure that such authorisation can be obtained promptly in all circumstances and is given in accordance with the law. Keeping good records, preferably against a pre-prepared checklist, will help to protect the investigator and the institution from any charge of improper or illegal action.

System and network administrators shall be made aware in their induction process 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, is likely to be considered by the University as gross misconduct.

Administrators must always work within the University's information security and data protection policies, which can be found at http://www.sussex.ac.uk/infosec and should seek at all time to follow professional codes of behaviour such as the following:

- ACM Code of Ethics and Professional Conduct

- FEANI's Code of Conduct for Professional Engineers
- BCS Code of Conduct and Code of Good Practice
- SAGE Code of Ethics
- SANS IT Code of Ethics

Authorisation and Authority

System and network administrators require formal authorisation from the "owners" of any systems 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 Sussex, the *Policy for Institutional Access to Information within University ICT Accounts, Equipment and Networks* delegates operational authority to the Director of IT Services who is usually the appropriate authority to grant authorisation to system administrators working on the University network. Authority for exceptional reasons must be given by the Chief Operating Officer.

Individual systems connected to the network may have more complicated ownership, as they may be formally the property of Schools or other divisions, but these Security Policies delegate overall authority to the Director of IT Services or the Chief Operating Officer. If any administrator is ever unsure about the authority they are working under then they should stop and seek advice immediately, as otherwise there is a risk that their actions may be in breach of the law.

Permitted Activities

The scope of this charter is divided into two principal 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, as is the investigation of crime.

The second area is where administrators may play a part in monitoring compliance with policies applying to systems. For example the University bans the use of Skype in supernode configuration. The JANET Acceptable Use Policy prohibits certain uses of the network.

> Here the administrator is acting in support of policies, rather than protecting the operation of the system.

The law differentiates between operational and policy actions, 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, authorised 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 relevant authorisation.

The administrator must ensure that these activities do not result in the loss or destruction of information. If a change is made to content 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

Managers must not ask, nor administrators act, to monitor or enforce policy unless sure that all reasonable efforts have been made to inform users both that such monitoring will be carried out and the policies that 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 authorised under the *Policy for Institutional Access to Information within University ICT Accounts, Equipment and Networks* 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 or by marking it as personal,

the administrator must not examine or attempt to make the content readable without specific authorisation from the appropriate authority 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 a users files 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

System and network administrators are required to respect the secrecy 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 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 the Director of IT Services (or, if this is not appropriate then a more senior authority) 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 inadvertently known to authorised administrators during the course of their investigations. Unexpected or unauthorised disclosure of information to third parties, particularly where this affects sensitive personal data, should be reported to the relevant data controller.

Intentional 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 appropriate authority, modify the contents of any file in such a way as to damage or destroy information.

Unintentional Modification of Data

Administrators must be aware of the unintended changes that their activities may make to systems and files. For example, listing the contents of a directory may well change the last accessed time of the directory and all the files it contains; other activities may well generate records in logfiles. This may destroy or at best confuse evidence that may be needed later in an investigation.

Where an investigation may result in disciplinary charges or legal action, great care must be taken to limit such unintended modifications as far as possible and to account for them. In such cases a detailed record should be kept of every command typed and action taken. If a case is likely to result in legal or disciplinary action, the evidence should first be preserved using accepted forensic techniques and any investigation performed on a second copy of this evidence.

Managed Services

It is increasingly common for organisations to use externally provided services. It is important for the commissioning organisation to be absolutely clear on its own role and that of the service provider with respect to the *Data Protection Act 1998* and other relevant legislation. The commissioning organisation must ensure that the service provider has appropriate controls in place to regulate the activities of its system administrators, and that clear joint procedures are in place for the handling of the situations outlined in this charter.

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

Guidelines to good forensic practice are available, for example

- NHS Forensic readiness guidelines
- CERT Co-ordination Center First Responders Guide to Computer Forensics (USA)

System Administrator's Charter – Examples

Examples

Modifying or deleting information

Mail loops/quota problems

Two common situations cause problems for electronic mail systems: users who attempt to forward incoming 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 authorised 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 the appropriate authority in compliance with the *Information Security Policies – Institutional Access*.

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 'notice and take-down procedure'. As there are likely to be legal implications for the organisation, takedown procedures should not be left to system administrators to write. Administrators receiving complaints about defamatory or copyright material on servers should always bring these to the attention of the appropriate authorities. File permissions can usually be changed to prevent further publication without destroying the information.

Using log files

Investigating service failures

The job of a system 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 authorised 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 appropriate authorities 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 data from cache and other logs should only be released through the proper procedure as laid out in section 22 of the Regulation of Investigatory Powers Act 2000. The police should provide a section 22 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. [Note that telling users that cache logs may be monitored may well act as a deterrent to inappropriate activity]. 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 system 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. General monitoring of screens and keyboards is currently a legally questionable area: sites wishing to implement it should study the Office of the Information Commissioner's Employment Practice Code (13MB PDF) and in particular Section 3 on Monitoring at Work. 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.

General

Discovering evidence of other breaches

It is quite common for authorised administrators to find 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. Administrators must not abuse the power and trust given to them by users and management.

Ownership:

Owner	Department/Team
Director ITS	ITS

Authors:

Author(s)	Department/Team
Jerry Niman	Consultant

Contributors and Reviewers:

Contributor/Reviewer	Department/Team
Matthew Trump	Information Service Assurance Manager

Revision History:

Version Number	Status D/R/A/I[1]	Date Issued	Reason for Issue	Issued by
1.0	A	16/2/2010	Approved by ISC	
1.1	R	8/1/2015	Updated links to external documents and references to internal policies. Added section on Managed Services	PD
2.0	I	3 March 2015	Approved by ISC	PD
2.1	I	20 June 2017	Minor Amendments	MT
2.2	I	12 Sept 2017	Change Registrar to COO	MT

[1] D = Draft; R= Ready for approval; A = Approved for issue; I = Issued