Published on *Jisc community* (https://community.jisc.ac.uk)

System Administrators Charter

System Administrators Charter

This document can now be found at https://repository.jisc.ac.uk/8369/1/suggested-charter-for-system-and-network-administrators.pdf [1]

Display as Single Column?:

Suggested Charter for System Administrators

Suggested Charter for System Administrators

This document has been prepared by Andrew Cormack, Chief Regulatory Adviser at Jisc Technologies. It is endorsed by the Universities and Colleges Information Systems Association (UCISA). Members of the UCISA Networking Group were closely consulted during the drafting process.

We hope that this charter will be useful to three groups: to users who wish to know the powers of administrators and to be assured that these will not be abused; to administrators themselves who are often concerned about the legality and implications of their actions; to managers to understand what are the reasonable requirements of the administrators' job and what activities they will be required to support.

Institutions will, of course, consult their legal advisers and make their own arrangements to comply with legislation. However, we suggest that this charter, or an equivalent statement of rights and responsibilities, should form part of the job description or job instructions of any person employed as a system or network administrator. We believe that this will go some way to compliance with the requirements for authorisation contained in the *Investigatory Powers Act 2016*, and for procedures to protect personal data contained in the *Data Protection Act 2018*.

Acceptance of the rights and privileges of authorised administrators should be a condition of use of any computer connected to a network and also of connecting

any computer to the network.

A Suggested Charter for System and Network Administrators

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 other users in their files, or sent by users over communications networks. This charter 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 charter and should be the subject of local working arrangements.

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 actions. Organisations should consider including additional safeguards - such as secure audit logs, oversight by a colleague, or separation of duties – in their procedures.

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 the system administration role doubtful, but is likely to be considered by their employers as gross misconduct. Administrators must always work within their organisation's information security and data protection policies, and should seek at all time to follow professional codes of behaviour such as the following:

- ACM Code of Ethics and Professional Conduct [9]
- BCS Code of Conduct and Code of Good Practice [10]

- Usenix System Administrator's Code of Ethics [11]
- SANS IT Code of Ethics [12]
- EthicsfIRST Ethics for Incident Response and Security Teams [13]

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 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.

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 a university or college this right is likely to be delegated by the organisation to the Head of IT, or equivalent function. This person is therefore usually the appropriate authority to grant authorisation to network administrators working on the college network. Individual systems connected to the network may have more complicated ownership, as they may be formally the property of departments or other divisions. Authority in these cases will need to be worked out locally, but it may be easiest to delegate authority to the Head of IT either as part of the agreement by which a computer is managed centrally, or as a condition of connecting to the network. This document will use the term "Head of IT" on the assumption that authority over all systems on the network has been granted to that post: institutions may replace this be an appropriate title of group to suit local circumstances.

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

- Operational activities [14]
- Policy activities [15]

The duties of system 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 as is the investigation of crime.

Many administrators also play a part in monitoring compliance with policies which apply to the systems. For example some organisations 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 45 of the *Investigatory Powers Act 2016*, 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 authorisation from the Head of IT 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 or by marking it as personal, the administrator must not examine or attempt to make the content readable without specific authorisation from the Head of IT 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

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 Head of IT (or, if this is not appropriate, to a senior manager of the organisation) 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 2018*) that is stored on their 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 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, particularly when dealing with Operational issues, where this is not possible. These are reflected in the different routine permissions for Operational and Policy investigations above: for Policy issues there should be sufficient time to seek authorisation to access personal filespace, and changing file ownership may be

sufficient to address the immediate issue. 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 will 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 the 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.

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 *Investigatory Powers Act 2016* in particular s.45 on Operational activities [16] and s.46 on Policy ones [17];
- The *Data Protection Act 2018* [18] and the General Data Protection Regulation [19];
- The *Human Rights Act 1998* [20].

The Office of the Information Commissioner's Employment Practice Code [21] (with quick guide [22]) includes a section on Monitoring at Work, including use of computers and networks.

Guidelines to good forensic practice are available, for example

- Association of Chief Police Officers (ACPO) Good Practice Guide for Computer Based Evidence [23];
- CERT Co-ordination Center First Responders Guide to Digital Forensics [24] (USA)

A selection of examples [25] have been written to illustrate how the charter might be applied to particular situations.

Version 1.5

Display as Single Column?:

System Administrators Charter - Examples

System Administrators Charter - Examples

The following examples have been chosen to accompany the System Administrator's Charter [26] to indicate how the charter is intended to work in practical situations.

As I receive enquiries about the charter I will try to update these examples, so if you find an interesting situation which is not covered here, or a case that makes the points better, then please let me know andrew.cormack@jisc.ac.uk [27].

Examples

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 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 internal authority, usually the Head of Information Services or equivalent.

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 internal authorities. File permissions can usually be changed to prevent further publication without destroying the information.

Using logfiles

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 internal 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 66 of the Investigatory Powers Act 2016 [28] and our Jisc Guide to disclosing information to law enforcement [29].

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 [21] (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.

Version 1.03

Display as Single Column?:

Source URL: https://community.jisc.ac.uk/library/janet-services-documentation/system-administrators-charter

Links
[1] https://repository.jisc.ac.uk/8369/1/suggested-charter-for-system-and-network-administrators.pdf
[2] http://www.ja.net/development/legal-and-regulatory/regulated-activities/charter-for-system-administrators.html#1
[3] http://www.ja.net/development/legal-and-regulatory/regulated-activities/charter-for-system-administrators.html#2
[4] http://www.ja.net/development/legal-and-regulatory/regulated-activities/charter-for-system-administrators.html#3
[5] http://www.ja.net/development/legal-and-regulatory/regulated-activities/charter-for-system-administrators.html#4
[6] http://www.ja.net/development/legal-and-regulatory/regulated-activities/charter-for-system-administrators.html#5
[7] http://www.ja.net/development/legal-and-regulatory/regulated-activities/charter-for-system-administrators.html#6
[8] http://www.ja.net/development/legal-and-regulatory/regulated-activities/charter-for-system-administrators.html#7
[9] http://www.acm.org/about-acm/code-of-ethics
[10] https://www.bcs.org/membership/become-a-member/bcs-code-of-conduct/
[11] https://www.usenix.org/system-administrators-code-ethics
[12] http://www.sans.org/resources/ethics.php
[13] https://ethicsfirst.org/
[14] http://www.ja.net/development/legal-and-regulatory/regulated-activities/charter-for-system-administrators.html#3a

[15] http://www.ja.net/development/legal-and-regulatory/regulated-activities/charter-for-system-administrators.html#3b
[16] https://www.legislation.gov.uk/ukpga/2016/25/section/45
[17] https://www.legislation.gov.uk/ukpga/2016/25/section/46
[18] https://www.legislation.gov.uk/ukpga/2018/12/contents
[19] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[20] http://www.legislation.gov.uk/ukpga/1998/42/contents
[21] https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf
[22] https://ico.org.uk/media/for-organisations/documents/1128/quick_guide_to_the_employment_practices_code.pdf
[23] http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
[24] http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=7251
[25] https://community.ja.net/library/janet-services-documentation/system-administrators-charter-examples
[26] https://community.ja.net/library/janet-services-documentation/suggested-charter-system-administrators
[27] mailto:andrew.cormack@jisc.ac.uk
[28] http://www.opsi.gov.uk/acts/acts2000/20000023.htm
[29] https://www.jisc.ac.uk/guides/networking-computers-and-the-law/disclosure-of-information-to-law-enforcement