University of Kent

Information Systems Privileged User Charter[i]

Many individuals have elevated permissions to varying degrees on some or all IT systems. Some of these permissions are only granted when required, others are granted implicitly by membership of certain groups. Individuals with elevated privileges are not restricted to staff within Information Services but are from across the University.

With these elevated privileges comes increased responsibility – all staff with elevated permissions will undergo training[1] in these responsibilities. Abuse of privileged status will be regarded as a serious disciplinary matter, and in some cases can be a criminal matter.

If and when staff leave the University, or are no longer a member of one or more of the membership groups, either through secondment or a permanent change in job these permissions will be revoked.

The University will from time to time audit the status of all members of staff and accounts with increased privilege and confirm that this is still required and at the correct level. All people with elevated privileges and their line managers are expected to be familiar with this charter, and this will be affirmed on a regular basis.

1. Introduction

System and network administrators[2], 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. For these reasons they will have elevated and privileged permissions. 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.

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.

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 the University's information security and data protection policies, and should seek at all times to follow professional codes of behaviour.

2. Authorisation and Authority

System and network administrators require formal authorisation from the 'owners' of any

[1] Deemed appropriate by line-manager

[2] "System and network administrators" applies to all those with 'elevated privileges' to a greater or lesser extent. This includes, but is not limited to, those in a departmental IT support role, through persons who 'look after' a specific system to people with University spanning access privileges.

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 right is delegated by the Vice Chancellor to the Director of Information Services. This document will use the term 'Designated Authority' which could refer to either of these posts, or other nominee, as is most appropriate.

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.

3. Permitted activities

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 an incident.

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 3(3) of the Regulation of Investigatory Powers Act 2000, 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.

3.1 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; or ownership (see Modification of Data below);
- Create relevant new files on those computers.
- Ensure system policy is in place.

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 Designated 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 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.

3.2 Policy activities

Administrators must not act to monitor or enforce a policy[3] 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.
- Ensure system policy is in place.

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 Designated 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 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.

4. Disclosure of information

System and network administrators are required to respect the secrecy of files and correspondence in accordance with Data Protection Act.

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 Designated Authority (or, if this is not appropriate, to a senior manager of the organisation) for them to decide whether further investigation is necessary.

[3] Policy(ies) and/or regulations which apply include, but are not necessarily limited to University of Kent regulations (`https://www.kent.ac.uk/is/regulations/it/` and `https://www.kent.ac.uk/regulations/general.html`, as amended from time to time) and those policies of third party systems which a user may be accessing.

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 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.

5. 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.

6. 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 any investigation, were an investigation to be necessary.

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.

[i] Charter is based on JANET wording https://community.ja.net/library/janet-services-documentation/suggested-charter-system-administrators