Ulster University Code of Practice Cover Sheet

Document Title	Systems Administrators Code of Practice 2.3
Custodian	ISD Heads
Approving Committee	ISD Committee
Policy approved date	2017-03-09
Policy effective from date	2017-03-09
Policy review date	2018-03-09

Changes to previous version
Page 1 – “charter” changed to “document” Page 3 – “an” changed to “a” Page 4 – “all of these” changed to “these” Page 4 – Deleted duplicate paragraph “Where the content of a file, database or communication appears to have been deliberately protected by the owner, for example by encrypting it, the Systems Administrator must not attempt to make the content readable without specific authorisation from management or the owner of the file or database.” Page 4 – “during the course” changed to “during” Page 5 " during the course of” changed to “during”

INTRODUCTION AND BACKGROUND

Systems Administrators, Network Administrators, Database Administrators and Database Developers (collectively referred to in this document as Systems 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 databases, or sent by users over communications networks. This code of practice sets out the actions of this kind which authorised Systems Administrators may expect to perform on a routine basis, and the responsibilities which they bear to protect information belonging to others. Systems 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 and should be the subject of local working arrangements.

On occasion, Systems Administrators may need to take actions beyond those described in this document. In all cases, they must seek individual authorisation from the appropriate person in their organisational unit 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. Organisational units 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.

Systems 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 administration role doubtful, but is likely to be considered by their employers as gross misconduct.

The term “database” may include the associated tables, structure, elements and permissions of the database, and the term “file” may include associated file structures and permissions.

Further information on ISD policies, standards and guidelines is available at:

http://www.ulster.ac.uk/isd/policies

RELEVANT LEGISLATION

The University will comply with all legislation and statutory requirements relevant to information and information systems, including:

- Computer Misuse Act 1990;
- Data Protection Act 1998;
- Communications Act 2003;
- Copyright, Designs and Patents Act 1988;
- Freedom of Information Act 2000;
- Human Rights Act 2000;
- Regulation of Investigatory Powers Act 2000;
- Police and Justice Act 2006;
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (‘the Lawful Business Regulations’)

AIMS, PURPOSE AND SCOPE OF THE CODE OF PRACTICE

The purpose of this document is to provide clear guidelines for members of the University who are Systems Administrators or who have been given elevated rights (administrator, admin, root or equivalent) to IT systems, to ensure a common, accountable, secure, and professional approach. Each person who is to be granted elevated rights is expected to read and commit to these codes of practice.

This document applies to all members of the University who are given Systems Administrator or equivalent elevated access privileges on any managed service or server.

CODE OF PRACTICE

Authorisation and Authority

Systems Administrators require formal authorisation from the "owners" of any equipment, systems or services they are responsible for. If any Systems Administrator is ever unsure about the authority they are working under they should stop and seek advice immediately as otherwise there is a risk that their actions may be in breach of this Code of Practice.

All Systems Administrators of ISD hosted systems are required to seek approval, gain authorisation and have their privileges recorded via the on-line system provided.

Responsibility

"Having responsibility" for equipment, systems or services means that a Systems Administrator is accountable for its successful operation, and being empowered to use experience, specialist skills, and judgement to make systems work in the most effective way. It does not mean that a Systems Administrator can make unilateral decisions about systems, or assume they are the only person who is permitted to, or capable of making decisions about the systems they administer. Communication is a critical element in administering all systems, and a competent Systems Administrator will, where possible, always review significant plans or changes with others.

Permitted Activities

The duties of Systems Administrators can be divided into two areas – operational activities and policy activities.

1. Operational Activities

The primary duty of a Systems 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 Systems Administrator is acting to protect the operation of the systems for which they are responsible.

Where necessary to ensure the proper operation of networks or computer systems for which they are responsible, authorised Systems 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 or databases 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 Systems Administrator must not attempt to make the content readable without specific authorisation from management or the owner of the file.

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

2. Policy Activities

Many Systems Administrators have a duty to monitor compliance with policies which apply to the systems. In these cases, the Systems Administrator is acting in support of policies, rather than protecting the operation of the system.

Systems 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 or database is examined, or a network communication monitored, individual permission must be obtained from all the owner(s) of files or databases, or all the parties involved in a network communication. The University maintains an IT Monitoring Policy and IT Monitoring Code of Practice with detailed information on permissible monitoring activity.

Provided Systems 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.

The Systems Administrator must ensure that these activities do not result in the loss or destruction of information. If a change is made to user file storage, 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 Administrators are required to respect the privacy of files, databases and correspondence.

During their activities, System 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 authorised investigation.

Information relating to a current investigation may be passed to managers or others involved in the investigation; information that emerges during the course of an investigation, but 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.

Systems 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 Systems Administrators during their investigations. Particularly where this affects sensitive personal data, any unexpected disclosure should be reported to the relevant data controller. A further explanation of sensitive and sensitive data can be found in the University's Protective Marking Standard.

Modification of Data

1. *Intentional Modification of Data*

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

- Rename or move files or databases, if necessary to a secure off-line archive, rather than deleting them;
- Instead of editing a file or database, move it to a different location and create a new file or database 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 or database 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 Systems Administrator may not, without specific individual authorisation from the appropriate authority, modify the contents of any file or database in such a way as to damage or destroy information.

2. *Unintentional Modification of Data*

Systems Administrators must be aware of the unintended changes that their activities will make to systems, files or databases. 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.

Creation of Accounts

Systems Administrators may have the capability to create user accounts on the systems they manage. They may only create accounts for individuals authorised by the University or the 'owner' of the system. Details on the creation, management, support and deactivation of user accounts is provided in the University's User Account and Access Policy and User Account Management Code of Practice.

Standards on user account passwords and authentication are provided in the Password Standard and Authentication Standard.

System Maintenance

- Systems should have the latest approved software and patches installed
- Systems should have all unnecessary services disabled, and an appropriately configured local firewall employed
- Systems should be protected from unauthorised access and modification
- Systems should have appropriate written data/disaster recovery and business continuity plans

OTHER RELEVANT POLICIES AND INFORMATION

- Password Standard
- Authentication Standard
- IT Monitoring Policy
- IT Monitoring Code of Practice
- User Account and Access Policy
- User Account Management Code of Practice
- Networks Standard
- Protective Marking Standard

ACKNOWLEGEMENTS

This document has consulted, and borrowed from the following documents:

- Code of Conduct for System Administrators, The University of Warwick
- Suggested Charter for Systems and Network Administrators, UKERNA/UCISA