University of Warwick
Code of Conduct for System Administrators
Version 1.2 (revision due to the introduction of the GDPR)

July 2019

1 Contents

2 References and Acknowledgement

This document is adapted from the 'Suggested Charter for Systems and Network Administrators' prepared by Andrew Cormack of UKERNA, in consultation with UCISA and published by the JNT Association for use by the HE community. JNT Association copyright is acknowledged.

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 Code of Practice together with the guidance contained in the Information Commissioner's Codes of Practice

https://ico.org.uk/

1. The Regulation of Investigatory Powers Act (2000) and the secondary Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

2. The General Data Protection Regulation (2018)

3. The Human Rights Act (1998)

In Addition System Administrators are bound by Reg.31 The use of University Computing Facilities.

3 Introduction

3.1 Background

Providing secure, high-availability, functionally-rich critical services in the Warwick environment is a challenging responsibility. The scope of legislation and general scrutiny which applies to data security and accountability has increased dramatically over the past few years to the point where our auditors have advised us to set out clear guidelines.

3.2 Scope

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

3.3 Purpose

The purpose of this document is to provide clear guidelines for members of the University who are Systems Administrators or 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 before rights are assigned.

4 Mandate

An individual who is granted elevated rights to IT systems is entrusted with operating the system or service on behalf of the University or Department, for the benefit of its members. An individual entrusted with this responsibility will always administer systems with this in mind.

5 Authorisation and Authority

System 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 the University of Warwick this right is delegated to the Director of IT Services, normally delegated to the appropriate Head of Service, to decide which members of IT Services need to be allowed System administrator status on any individual system or service, or a range of services, and when it is appropriate to change the ownership and scope of responsibility.

The Head of Department is usually the person with authority for departmentally provided services.

If any 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 law.

6 Responsibility

'Having responsibility' for an IT system, server, or service, means that a System 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 system 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 System administrator will, where possible, always review significant plans or changes with others.

7 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 crime.

Many administrators have a duty to monitor compliance with policies which apply to the systems. For example, 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.

7.1 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 (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.

7.2 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. The University publishes a statement on the Regulation of Investigatory Powers Act informing users of the circumstances in which the University may monitor electronic communications. This statement is available on the IT Services web site..

Version 1.1

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.

7.3 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 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.

Administrators must be aware of the need to protect the privacy of personal data and special category data (within the meaning of the General Data Protection Regulation 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 Data Protection Officer (DPO) using the breach report form located at
https://warwick.ac.uk/services/idc/dataprotection/breaches

7.4 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.

7.5 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. Authorised users will normally be restricted to members of the University (ie staff, students, or others categories of member approved by the Registrar)

8 Practice

Departments are encouraged to append to this document local working practices which detail how this Code of Practice is to be implemented for carrying out day-to-day work. IT Services can provide advice, and there should be appropriate consultation.