UNIVERSITY OF PORTSMOUTH

CHARTER FOR SYSTEM AND NETWORK ADMINISTRATORS

March 2016

Contents

Document title		
Normal text		
Document author and department		
Normal text		
Approving body		
Normal text		
Date of approval		
Normal text		
Review date		
Normal text		
Edition no.		
Normal text		
ID Code		
Normal text		
Date of effect		
Normal text		
EITHER For public access online (internet)? Tick as appropriate		**YES**
For public access on request copy to be mailed Tick as appropriate	**NO**	**YES**
OR For staff access only (intranet)? Tick as appropriate		**YES**
Password protected Tick as appropriate	**NO**	**YES**
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk		

If you need this document in an alternative format, please email corporate.communications@port.ac.uk

The latest version of this document is always to be found at:

https://erecords.port.ac.uk/documents/qA43279

Summary

What is this document about?

IT system and network administrators (aka 'admins') must use privileged accounts to carry out their duties and must remain aware that the privileges they have place them in a position of considerable trust.

The charter acts as a safeguard for admins and users by setting out the responsibilities which admins have to protect information and by describing the reasonable activities they might be asked to perform.

If a system or network administrators is ever unsure about the authority under which they work, or the ethical or legal basis for what they have been asked to do, then they must stop and seek advice.

Important: Unauthorised surveillance is a criminal offence under the Regulation of Investigatory Powers Act 2000 and could also be regarded as 'interference with an individual's privacy' under the the Human Rights Act 1998

Who is this for?

This IS advisory is aimed at those staff who administer and manage information systems.

How does the University check this is followed?

Annual review of this IS advisory will be performed to evaluate its effectiveness.

Who can you contact if you have any queries about this document?

Any questions about should be directed to servicedesk@port.ac.uk

1.0 Scope

This charter applies to members of staff with privileged access to computer systems who perform the role of system or network administrators (aka 'admins'). Administrators of IT systems which are not under the support of Information Services should also adopt this charter.

2.0 Responsibilities

Admin accounts will only be provided to trained and experienced members of the University who maintain the highest standards of professionalism and due respect for confidentiality and individual privacy.

2.1 An annual review of admin accounts is recommended. Unused accounts must be safely disabled/locked to avoid compromise.

The Director of Information Services is authorised to request an investigation and to specify the area under investigation and what actions might be a reasonable.

3.0 Aims and Objectives

The duties of administrators can be divided into two areas – Operations and Policy.

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.

4.0 Operational Actions (e.g. ordinary, day to day tasks):

The operational duty of an administrator is to ensure that networks, systems and services are available to users and that information is processed and transferred correctly. For example, they may install new software, upgrade existing systems, make backups, restore files from backup, recover accounts, reset passwords and maintain systems. This list is not definitive and other operational tasks may be performed.

The administrator must ensure that operational activities do not result in the loss or destruction of information.

As far as is reasonably practical, admins should normally inform any affected parties beforehand if the operational task is likely to cause disruption or data loss.

4.1 Policy Actions (e.g. investigation, audit/compliance checking):

Administrators may also monitor compliance with policies. The University Acceptable Use Policy and the JANET Acceptable Use Policy both prohibit certain uses of the network.

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.

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 Director of Information Services or the owner of the file.

4.2 Disclosure of information

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 an investigation must be passed directly to managers involved in the investigation.

Information must only be disclosed if it is thought to indicate an operational problem, or a breach of local policy or the law. Where a breach of law is suspected, the Director of IT or a senior manager of the organisation must be informed.

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 or routine activities.

Any unexpected or accidental exposure of personal data should be reported to the Security Architect.

4.3 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.

Administrators may:

- Rename or move files, if necessary to a secure off-line archive;
- Relocate 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).

4.4 Unintentional Modification of Data

Administrators must be aware that any unintended changes to systems and files may destroy or damage evidence that may be needed as part of an investigation.

Where an investigation may result in disciplinary charges or legal action, great care must be taken to limit such unintended modifications and to account for them. A detailed record should be kept of every command typed in and every 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.

If in any doubt about the legitimacy of an action, admins must obtain authorisation from the appropriate person for the specific action they need to take.

References:

The following Acts are particularly relevant to the activities covered by this charter.

- The Regulation of Investigatory Powers Act 2000
- The 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 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 Good Practice Guide for Computer Based Evidence

JISCLegal technical investigation process

University of Portsmouth
Department of Human Resources
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3141
F: +44 (0)23 9284 3122
E: university.secretary@port.ac.uk
W: www.port.ac.uk