UNIVERSITY OF PORTSMOUTH

PRIVILEGED ACCESS

Jan 2020

Contents

Summary 4

Who is this for? 4

How does the University check this is followed? 4

Who can you contact if you have any queries about this document? 4

1.0 Introduction 5

2.0 The Use of Three-Letter Privileged Accounts (TLAs) 5

3.0 Transparency and Safeguarding 5

4.0 The management of privileged access 6

5.0 Process when an administrator leaves or transfers 6

6.0 Responsibilities, duties, and tasks of account holders 6

Document title
Privileged Access
Document author and department
R Walker IS
Approving body
IS
Date of approval
Jan 2020
Review date
Jan 2021

Edition no.	
1	
ID Code	
Date of effect	
June 2020	
EITHER For public access online (internet)? Tick as appropriate	**NO**
For public access on request copy to be mailed Tick as appropriate	**YES**
OR For staff access only (intranet)? Tick as appropriate	**YES**
Password protected Tick as appropriate	**NO**
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

Summary

This advisory sets out the management controls relating to privileged access.

Privileged access is defined as access to the UoP IT infrastructure that enables the individual to take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users.

Who is this for?

This IS advisory is intended for staff who manage and administer UoP information systems. Privileged access is typically granted to system administrators, network administrators, and/or employees whose job duties require elevated powers, rights and privileges over a computing system or network.

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 this advisory should be directed to servicedesk@port.ac.uk

1.0 Introduction

1.1 Privileged access is defined as access to the UoP IT infrastructure that enables the individual to take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users.

1.2 Privileged access is typically granted to system administrators, network administrators, and/or employees whose job duties require elevated powers, rights and privileges over a computing system or network.

1.3 Individuals with privileged access must respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with any relevant laws or regulations. Individuals also have an obligation to keep themselves informed regarding any procedures, business practices, and operational guidelines pertaining to the activities of their local department.

2.0 The Use of Three-Letter Privileged Accounts (TLAs)

2.1 Some staff require the use of accounts with wide-ranging rights to the systems and networks - these are referred to as “three letter accounts” (TLA). TLA accounts must only be used to carry our administrative tasks and *not* for conventional computing - like reading email or web browsing.

2.2 Given the increased risks from ransomware - where attackers will not just encrypt data but attempt to steal it for future blackmail - it is critical that these accounts are restricted to the use for which they were intended.

2.3 Privileged accounts with administrator rights to all or part of the university network (i.e. “three letter accounts”) must :-

2.3.1 Be protected with a long (> 15 charters) and strong password.

2.3.2 Where feasible should be protected with multi-factor authentication.

2.3.3 Only be used for the purposes for which rights are required; The following uses are prohibited :-

a. Logging into the VPN.
b. Browsing the Internet.
c. Reading emails.
d. Any other non-privileged computing activity.

2.1 Operational duties and areas of responsibility should be appropriately segregated to reduce the risk and consequential impact of information security incidents.

3.0 Transparency and Safeguarding

IT system and network administrators 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. A Charter for Administrators has been created which acts as a safeguard for administrators and provides transparency by setting out the responsibilities which administrators have to protect information and by describing the reasonable activities they might be asked to perform.

4.0 The management of privileged access

4.1 Privileged access is granted only to authorised individuals.

4.2 Privileged access can only be granted by EPS managers.

4.3 MFA will be implemented on all administrator accounts where possible.

4.4 VPN access must be used for remote access to a privileged account.

4.5 A self-documenting inventory of privileged accounts is maintained

4.6 Privileged access may be used only to perform assigned job duties.

4.7 Standard user accounts will not be granted with privileged account status.

4.8 Privileged accounts will be reviewed every 6 months by the responsible manager

4.9 Privileged accounts will be reviewed after a relevant security incident or alert

4.10 Privileged accounts will be reviewed following a change of staff role or function

4.11 Privileged accounts will be reviewed on departure or transfer of staff member

4.12 Privileged accounts reviews will be carried out by the responsible manager

5.0 Process when an administrator leaves or transfers

5.1 Review the account holdings of that individual

5.2 Change the password on affected accounts

5.3 Update the relevant password to the repository

6.0 Responsibilities, duties, and tasks of account holders

6.1 Privileged account holders must notify management if they believe that the privileges on their account are excessive or unnecessary.

6.2 If a system administrator is 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 management approval.

6.3 If an action can be carried out without privileged access, then other (non-privileged) methods are to be used.

6.4 Privileged access may be used to grant, change, or deny resources, access, or privilege to another individual only for authorised account management activities or under exceptional circumstances. Such actions must be authorised and follow any existing organisational guidelines and procedures.

Examples include:

- Disabling an account apparently responsible for serious misuse such as: attempting to compromise root (UNIX/Linux) or the administrator account
- Disconnecting a host or subnet from the network when a security compromise is suspected;
- Accessing files on behalf of law enforcement authorities.
- Running security analysis software

Privileged access may be used to perform standard system-related tasks and duties on computers and networks as part of an authorised job role.

Examples include:

- Installing system software
- Upgrade existing systems
- Making backups and restoring files from backup
- Account recovery
- Granting and revoking access to systems
- Resetting passwords
- Systems maintenance and patching
- Searching through an email account
- Monitoring server performance

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