ISD Privileged Account Management Policy

Author: Tim Purkiss

Date: 9 Jun 2017

Version: 1.0

**Review/Revision History**

This document shall be reviewed annually or more frequently if required, e.g. following changes to related requirements, or to related documents.

| **Revision No.** | **Revision Date** | **Summary of Changes** | **Who** | **Changes marked** |
| --- | --- | --- | --- | --- |
| 0.1 | 9 Jun. 2017 | First draft | Bridget Kenyon | N/A |
|  |  |  |  |  |

**Approvals**

This document requires the following approvals

| **Name** | **Signature** | **Title** | **Date of Issue** | **Version** |
| --- | --- | --- | --- | --- |
| Mike Cope |  | Director, ISD |  | 0.1 |
| James McCafferty |  | Director of IT Service Delivery, and Deputy Director of ISD |  | 0.1 |
| Bridget Kenyon |  | Head of Information Security |  | 0.1 |

**Distribution**

This document has been distributed to:

| **Name** | **Date of Issue** | **Version** |
| --- | --- | --- |
| James McCafferty | 9 Jun 2017 | 0.1 |
| Andrew Dawson | 9 Jun 2017 | 0.1 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1. Introduction 4](#_Toc484787768)

[2. Scope 4](#_Toc484787769)

[3. Dependencies 5](#_Toc484787770)

[4. Related requirements 5](#_Toc484787771)

[5. Stakeholders 5](#_Toc484787772)

[6. Accountable Roles 5](#_Toc484787773)

[7. Definitions 6](#_Toc484787774)

[8. Policy statements 6](#_Toc484787775)

[8.1. Authorisation 6](#_Toc484787776)

[8.2. Usage 6](#_Toc484787777)

[8.3. Retention 6](#_Toc484787778)

[8.4. Documentation 6](#_Toc484787779)

[8.5. Monitoring 6](#_Toc484787780)

[8.6. Review 7](#_Toc484787781)

[8.7. Non-compliance 7](#_Toc484787782)

[9. Sanctions 7](#_Toc484787783)

# **Introduction**

Privileged accounts, by definition, allow their users to perform actions over and above the standard actions available to a normal user account. As such, it is vital that these accounts are maintained, reviewed and removed in a timely fashion. This maintenance prevents them from being left active inappropriately, with the consequent risk of misuse by a user who no longer requires access (or has left), or increased risk of compromise by an external attacker.

This document describes how ISD shall manage privileged accounts on systems for which it is responsible.

# **Scope**

This policy applies to:

* Accounts on servers, network equipment and other electronic devices managed by ISD
* All privileged accounts, including operating system, hypervisor, application, and network device.
* Any server that ISD manages[[1]](#footnote-1) or is responsible for, including servers which are managed by third parties on behalf of ISD.
* Any software on these servers. In this document, “software” shall be taken to include firmware, BIOS, hypervisor, operating system, driver, library, middleware, application, service, and other digital capabilities.

# **Dependencies**

Documents which rely upon this policy:

* Vulnerability Management Guidance for ISD servers.

Documents which this policy relies on:

* UCL Policy on Connecting Equipment to the College Network
<https://www.ucl.ac.uk/informationsecurity/policy/public-policy/Connection>
* UCL Information Security Policy
<https://www.ucl.ac.uk/informationsecurity/policy/public-policy/Policy>

# **Related requirements**

The UCL Network Connection Policy Clause 1.7 requires all UCL network-connected systems to be supported and up to date with security patches (updates).

The Data Protection Act Principle 7 states that “Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data…”.

# **Stakeholders**

The following roles, or their nominated representatives, should be involved in the review of this document.

* Head of Information Security
* Head(s) of ISD Server Management team(s)
* Service Owner(s) for Server Service(s)
* Chair of Security Working Group

# Accountable Roles

Department Heads shall ensure that servers and/or software which are managed by their staff are compliant with this policy.

Service Operational Managers shall ensure that systems which support their service are compliant with this policy, but may delegate operational activities to members of their Service Virtual Teams.

Service Operational Managers will ensure that the responsibilities of System Custodians as defined within this policy, the Information Security Policy, secondary policies and guidelines will be met.

Service Owners are ultimately accountable for the security of their service.

# **Definitions**

**Privileged accounts:** accounts which permit super-user access, or access allowing actions greater than those granted to standard accounts. These accounts may be tied to a user, or to an application.

**Privileged account custodian (PAC):** the individual who is responsible for the usage of a specific privileged account.

Also see [Glossary](https://www.ucl.ac.uk/informationsecurity/policy/public-policy/Glossary).

# **Policy statements**

## Authorisation

1. Only authorised PACs (privileged account custodians) shall be permitted to hold privileged accounts.
2. Authorisations shall be specific to a given privileged account[[2]](#footnote-2).
3. Each PAC shall be authorised (or de-authorised) by their line manager and the system custodian.
4. The Service Owner is responsible for specifying any additional rules relating to the authorisations process for systems supporting their service (e.g. background checks for certain services).
5. Privileged Accounts must not be shared[[3]](#footnote-3)
6. Authorisations should be based on a valid business requirement and time limited.

## Usage

1. Privileged accounts shall be used by their assigned PAC only.
2. Passwords for privileged accounts shall not be shared; only the PAC shall know the password.
3. Line managers are responsible for ensuring that accounts are used in compliance with UCL policies.
4. Passwords for privileged accounts shall be of a strength suitable for their intended purpose, based on the Service Risk Assessment.

## Retention

1. Privileged accounts which are no longer required shall be disabled immediately, and deleted within three months.
2. <Check what the Password and Account policies say about password changes on service accounts and sysadmin accounts> Passwords for privileged accounts shall be changed no less often than once per 150 days.
3. Service Owners are responsible for approving password lifespans for systems supporting their service, based on their Service Risk Assessment.

## Documentation

1. The system custodian shall manage and maintain records of authorised PACs, which shall indicate their name, role, and justification for privileged access, system(s) to which they have privileged access, date of authorisation and details of the authorising role.
2. The system custodian shall manage and maintain a record of reviews of access rights.
3. Records shall be stored in a location agreed between the system custodian and their line manager.

## Monitoring

1. All privileged account usage shall be logged.
2. Logs of privileged account usage shall be stored in a location to which the PAC does not have access.

## Review

1. Privileged accounts shall be reviewed by the system custodian at least every 6 months to verify that:
2. Accounts are still required
3. Access is only available to authorised PACs
4. Authorisations are valid
5. SOMs shall annually check records to ensure that reviews have been carried out for all of the systems supporting their service, and that processes have been followed appropriately.

## Non-compliance

1. Non-compliance shall be followed up by the relevant line manager in combination with the SOM(s) affected.
2. Serious non-compliance, including that affecting systems holding personal data or data classified at Highly Confidential, shall also be reported to the Information Security Group.

# **Sanctions**

This policy statement does not form part of a formal contract of employment with UCL, but it is a condition of employment that employees will abide by the regulations and policies made by UCL.

1. Including maintenance, upgrades, etc. [↑](#footnote-ref-1)
2. No blanket authorisations e.g. “root privilege for all Linux systems”. [↑](#footnote-ref-2)
3. For instance, the root account cannot be used to provide a group of staff privileged access. Each person needs a separate privileged account. [↑](#footnote-ref-3)