Policy: ISD Log Retention and Management

Author: Andrew Dawson and Bridget Kenyon

Date: 20 September 2010

Version: 1.0

Policy owner

| **From date** | **Who** | **Role** |
| --- | --- | --- |
| 20 Sept. 2010 | James McCafferty | Director of IT Service Delivery, and Deputy Director of ISD |
|  |  |  |

Revision History

| **Revision No.** | **Revision Date** | **Summary of Changes** | **Who** | **Changes marked** |
| --- | --- | --- | --- | --- |
| 0.1 | 20 Sept. 2010 | First draft |  |  |
|  |  |  |  |  |

Approvals

This document requires the following approvals

| **Name** | **Signature** | **Title** | **Date of Issue** | **Version** |
| --- | --- | --- | --- | --- |
| Mike Cope |  | Director, ISD |  | 0.1 |

Distribution

This document has been distributed to:

| **Name** | **Date of Issue** | **Version** |
| --- | --- | --- |
| Mike Cope | 20 April 2010 | 0.1 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1. Review plan 4](#_Toc500920297)

[2. Introduction 4](#_Toc500920298)

[3. Scope 4](#_Toc500920299)

[4. Dependencies 4](#_Toc500920300)

[5. Related requirements 4](#_Toc500920301)

[6. Stakeholders 4](#_Toc500920302)

[6.1. Accountable Roles 5](#_Toc500920303)

[7. Definitions 5](#_Toc500920304)

[8. Policy statements 5](#_Toc500920305)

[9. Sanctions 5](#_Toc500920306)

# **Review plan**

This document will be reviewed every year, or more frequently if required, e.g. following changes to related requirements, or to related documents.

# **Introduction**

ISD’s IT infrastructure provides a number of services to the UCL community and beyond. In the process of providing these services, a number of logs are generated. These have a number of purposes including recording access and attempted access, maintaining an audit trail, provision of debugging information for troubleshooting, etc. Depending on the purpose of the logs, they need to be retained for a period of time. There is an external expectation of being able to identify usage and attempted usage of systems for a reasonable period of time after the event. However, where logged information relates to the activities of living individuals, there is a competing requirement to not retain the information any longer than necessary.

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

# **Scope**

This policy applies to:

* Any system that ISD manages[[1]](#footnote-1) or is responsible for, including systems which are managed by third parties on behalf of ISD.

# **Dependencies**

Documents which this policy relies on:

* UCL Information Security Policy   
  <https://www.ucl.ac.uk/informationsecurity/policy/public-policy/Policy>
* UCL Records Retention Schedule  
  <http://www.ucl.ac.uk/library/docs/retention-schedule.pdf>

Documents which rely upon this policy:

* None at present

# **Related requirements**

The Data Protection Act Principle 5 states that “Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.” The Act does not set out any specific minimum or maximum periods for retaining 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 and Client Platform Service(s)
* Chair of Security Working Group

## Accountable Roles

Department Heads shall ensure that systems which are managed by their staff are compliant with this policy.

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

# **Definitions**

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

# **Policy statements**

* Systems logs providing an auditable record of activity and attempted activity shall be retained for a period of 6 months. This includes operating system logs, application software logs and usage reports, network traffic logs and exception files produced during network and email use.
* Access to logs shall be restricted to the custodian of the system and any other individuals with a legitimate need to access them.
* Logs shall be securely removed when no longer required.
* Logs shall be reviewed at an appropriate period to identify unauthorised and unusual activity patterns. Any such activity shall be reported to UCL’s Information Security Group. Where logs are voluminous it may be appropriate for the review to be done using automated software tools.
* Systems shall be appropriately sized to ensure that they have adequate capacity to accurately collect and retain logging information.
* Logs shall be appropriately backed-up and/or copied into a central log repository in a timely fashion. This applies particularly to client systems that are regularly re-installed.
* Log files stored on the central log repository shall not be able to be changed by the administrators of the systems which generate the logs.
* Where logs are post-processed to extract relevant information (e.g. where the logs are too voluminous to retain in their entirety for the full retention period), they shall be reviewed before deletion of the originating log record (or the automated process will be reviewed before implementation or change) to ensure that useful information is not discarded in the process.

# **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)