UK Longitudinal Linkage Collaboration

Population Health Sciences

Bristol Medical School

Canynge Hall

39 Whatley Road

Bristol BS8 2PS

UK Longitudinal Linkage Collaboration (UK LLC)

AUDIT POLICY

PUBLIC

Version 1.2

17 May 2023

Policy number:	POL-ISM-010	**Version:**	V1.2
Author:	Katharine Evans, Governance & Policy Manager	**Date:**	11/10/2022
Authorised by:	Andy Boyd, Director	**Date:**	13/12/2022
Date published:	13/12/2022	**Date to review:**	17/05/2024
Permission to edit this policy must be provided by:	Director; Senior Data Manager; Governance & Policy Manager		

Review History

Version:	Review Date:	Reviewed by:	Section(s) amended:	Authorised by:
V1.1	13/02/2023	Katharine Evans, Governance & Policy Manager	1.3 – added an expectation; 4 & 5.4 – added ref to UKSA RAP 5.1.1 – added a new spot audit and expanded on another	Andy Boyd, Director
V1.2	17/05/2023	Katharine Evans, Governance & Policy Manager	1 – updated DEA accreditation	Andy Boyd, Director

Contents – UK LLC Audit Policy

1. INTRODUCTION

1.1 Background

The UK Longitudinal Linkage Collaboration (UK LLC) organisation is led by the University of Bristol (UoB) and operated in collaboration with the University of Edinburgh (UoE).

The UK LLC holds **de-personalised data** about **Longitudinal Population Study (LPS) participants** in the **UK LLC Trusted Research Environment (TRE).**

The UK LLC has achieved **ISO 27001 certification**, completes the annual **NHS Data Security and Protection Toolkit** (DSPT) and has been accredited by the **UK Statistics Authority as a processing environment under the Digital Economy Act (DEA)**.

This policy will be reviewed to respond to any changes in the UK LLC risk assessment or risk treatment plan and at least annually.

1.2 Purpose

The UK LLC conducts regular audits in the spirit of continuous improvement of the UK LLC's Information Security Management System (ISMS) and continued compliance with ISO 27001, DSPT and DEA controls. The audits fall into three categories:

1. UK LLC internal **spot audits**.
2. UK LLC internal **detailed audits**.
3. UK LLC **supplier audits**.

Further information for UK LLC staff is available in the Audit SOP and Programme (SOP-ISM-011).

Prospective researchers and researchers already active in the UK LLC TRE can find further information in the Data Access and Acceptable Use Policy and also in the TRE User Guide available on the Resources for Researchers SharePoint. Specific enquiries can be emailed to access@ukllc.ac.uk

1.3 Expectations of Approved Researchers

Key to this policy, approved researchers understand that they must:

1. Achieve **ONS Accredited Researcher (AR) status** before they can access the UK LLC TRE and understand that if their ONS AR status expires, their access will be terminated.
2. Agree to adhere to all **project-specific terms and conditions**.
3. Ensure that all **analyses fall within the scope of their approved project** and to contact the UK LLC (access@ukllc.ac.uk) if they have any concerns regarding scope.
4. Ensure that any code developed does **not attempt to increase the risk of identifying UK LLC participants**.
5. Agree to their **ONS AR accreditation** and the **scope and content of their approved projects** being **audited** by the UK LLC.

2. SCOPE

This policy applies to all UK LLC staff, all suppliers and all researchers who are approved to access data in the UK LLC TRE for the purposes of their approved project(s).

3. ABBREVIATIONS

AR	Approved Researcher
DAA	Data Access Agreement
DURA	Data User Responsibility Agreement
ISMS	Information Security Management System
LPS	Longitudinal Population Study
OMG	Operational Management Group
ONS	Office for National Statistics
TRE	Trusted Research Environment
UoB	University of Bristol
UoE	University of Edinburgh

4. ROLES AND RESPONSIBILITIES

Who	What & Why
UK LLC Information Security Team	Oversees the implementation and maintenance of the UK LLC's ISMS and all related certifications and accreditations. Designs, co-ordinates and ensures adherence to the UK LLC's audit programme. If appropriate, escalates events/incidents to the Accrediting Body.
UK LLC Applications Team	Assesses all researchers and their applications against the Five Safes Framework. This includes checking ONS AR status, overseeing and documenting the multi-stage approvals process and coordinating completion of all the required paperwork, including Data Access Agreements (DAAs) and Data User Responsibility Agreements (DURAs).
UK LLC Data Team	Manages access to the UK LLC TRE and conducts regular spot audits of approved users and their projects.
Approved researchers	Researchers are bound by the conditions detailed in the Data Access and Acceptable Use Policy, in the DAA that covers their project and in the DURA that each approved researcher must sign before they are permitted access to the UK LLC TRE. They must ensure that they maintain their AR status for the duration of their time in the TRE, that all analyses fall within the scope of their approved project(s), that all project-specific terms and conditions are adhered to, and that any code developed is 'safe'.

5. UK LLC AUDITS

5.1 Types of audits

5.1.1 Spot audits

Spot audits should be scheduled at least once a year. The frequency and format of spot audits will be reviewed where non-conformities, events or breaches have been identified. Spot audits are carried out by UK LLC staff and include:

5.1.1.1 UK LLC

- **Physical security** – checking that access to the office is restricted to UK LLC staff
- **Clear desk and clear screen** – checking that staff lock their screens and put away paperwork when away from their desks
- **Understanding information security** – using a survey to test staff understanding of UK LLC information security policies and practices
- **Access permissions** – checking that access to files, mailboxes and the TRE is restricted to staff with a business need
- **Back-ups** – checking that all files and the UK LLC TRE are backed up
- **Quality of the Accredited Researcher Database** – checking that the database is up to date, complete and accurate
- **Quality of the Data Register** – checking that the register is up to date, complete and accurate
- **Quality of the Contracts Register** – checking that the register is up to date, complete and accurate
- **Patches and encryption of hardware** – checking that all laptops and desktops used by UK LLC staff are patched and encrypted.

5.1.1.2 Researchers and their projects in the TRE

- **Access permissions** – checking that access to the TRE is restricted to accredited researchers who have the necessary and appropriate permissions, i.e. valid ONS AR status, a signed DURA and a DAA that covers them
- **Scope and content of approved projects** – checking that researchers' analyses fall within the scope of the approved project, that they only have access to datasets approved by the data owners, that they are adhering to all project-specific terms and conditions, and that any code developed does not attempt to increase the risk of identifying UK LLC participants.

5.1.2 UK LLC team audits

Audits of each UK LLC team are planned provisionally to work in tandem with the triennial external ISO 27001 audit schedule – every UK LLC operational team will be internally audited at least once over the three-year period. The frequency of audits will be increased where a team conducts work of particular importance or of high risk. Audit frequency will be reviewed where a team has had non-conformities identified or where the team has experienced information security events/breaches.

5.1.3 Supplier audits

The UK LLC audits internal UoB suppliers, e.g. HR, IT Services. All external suppliers who provide information processing services to the UK LLC under contract are also within scope. However, external suppliers that can demonstrate current ISO 27001 certification and DEA accreditation – where the scope of the certification/accreditation covers the processing activities required by the UK LLC – can be exempted from UK LLC audit on the basis that their external certification/accreditation programme is providing effective audit and follow-up on control compliance.

Supplier audits are planned provisionally to work in tandem with the triennial external ISO 27001 audit schedule. Every internal supplier will be audited at least once over a three year period. Every external supplier providing data processing for the UK LLC (without ISO 27001 and DEA accreditation) will also be audited at least once over a three year period. The frequency of audits will be increased where the supplier conducts work of particular importance or of high risk. The audit frequency will be reviewed where a supplier has had non-conformities identified or where the organisation has been subject to information security events/breaches.

5.2 Audit preparation

5.2.1 Spot audits

The UK LLC Information Security Team (IST) will allocate a UK LLC auditor to each audit. The auditor reviews the steps detailed in the UK LLC Audit SOP and Programme (SOP-ISM-011).

5.2.2 Team and supplier audits

The UK LLC IST will allocate a UK LLC auditor to each audit, with consideration that the review should be conducted by a member of staff who:

- Is independent from the team to be reviewed
- Has undertaken sufficient training and/or has sufficient experience to conduct an objective and impartial assessment.

The IST will provide the auditor with prior audit findings and/or information regarding information security events, incidents or breaches. The auditor should define the audit objectives and scope in advance of the audit – these will be informed by the nature of the team/supplier, previous audit findings, the UK LLC ISMS, and ISO 27001 and DEA controls. Audits are conducted on a sample basis and auditors do not need to audit all controls.

Prior to the UK LLC Team audit/supplier audit, the auditor will provide the auditee with the UK LLC Audit Guide for Auditees (DOC-ISM-011) and will outline the audit plan which includes:

- The audit objectives and scope
- Auditor(s)
- The time, date and location of the audit
- What will happen after the audit, including how the findings will be used.

5.3 Audit execution and reporting

5.3.1 Spot audits

The auditor will conduct the audit as detailed in the UK LLC Audit SOP and Programme (SOP-ISM-011) and will submit a report to the UK LLC IST.

5.3.2 Team and supplier audits

The auditor will:

- Impartially and objectively assess if activities conform to UK LLC ISMS requirements, and ISO 27001, DSPT and DEA controls
- Record their findings using the UK LLC Audit Report Template (DOC-ISM-012), noting any positive or negative observations and if there are any non-conformities
- Provide the report to the auditee for them to correct any inaccuracies or provide additional information
- Provide a copy of the final report to the auditee and the UK LLC IST.

5.4 Audit outcomes

Where issues that require action by auditees or researchers are identified, the IST will send a corrective action plan, which should:

- Identify the root cause of a non-conformity
- Define the corrective action, who is responsible for achieving this and the date by which the action will be completed.

If the auditee or researcher responds in a satisfactory manner, the audit will be considered closed. If not, the UK LLC may take further action, including a wider investigation of the auditee's/researcher's activities. For researchers, access to the TRE may be suspended until the issue is resolved satisfactorily and serious breaches of UK LLC policy may lead to further penalties, as outlined in the UK LLC DAA and UK LLC Data Access and Acceptable Use Policy. If any non-compliances have been identified, the IST will consider whether an Information Security Case Report should be completed and submitted to the UK LLC Operational Management Group (OMG) for their consideration and approval. If appropriate, the IST will escalate non-compliances to the UK Statistics Authority's Research Accreditation Panel (RAP) (Research.Accreditation@statistics.gov.uk). If required, the UK LLC Risk Register will be updated.

5.5 Audit reporting

The UK LLC IST will collate audit findings, including trends in non-conformities, in a quarterly report (one of which comprises the ISMS annual review report) submitted to the UK LLC OMG for review.

6. RELATED DOCUMENTS

- UK LLC Information Security Policy – POL-ISM-001
- UK LLC Data Access and Acceptable Use Policy – POL-ISM-003
- UK LLC Audit SOP and Programme – SOP-ISM-011
- UK LLC Audit Guide for Auditees – DOC-ISM-011
- UK LLC Audit Report Template – DOC-ISM-012.