LSE Research Laboratory Data Security Standards: Secondary Data

Description: The London School of Economics Research Laboratory standards for access and use of secondary data for research.

Introduction

1. The availability of secondary data resources underpins the LSE Research Laboratory's (RLAB) research programme. Therefore, the security, confidentiality and good management of data resources is key to the success of the RLAB. Failure to secure data increases the risk of legal sanctions and reputational loss from which it may be difficult to recover.

Purpose

2. This document outlines the standards implemented by the LSE Research Laboratory (RLAB) to support the secure storage and use of research data.

3. This document also defines roles and responsibilities that relate to the implementation of these standards.

Scope

4. These standards are applicable to, and will be communicated to, all members of the RLAB including (but not restricted to) staff, students, visitors and associates.

5. For the purposes of this document, the RLAB includes the following research centres: CASE, CVER, CEP, STICERD and the What Works Centres.

6. Research data in this context is defined as observational, experimental, simulated, derived or compiled resources that a researcher is accessing for the purposes of their research (e.g., survey data, administrative data, images, video or audio files, computer files etc).

7. The data covered by these standards are anonymised data, which offer little possibility for the user to disclose sensitive information (even in combination with other sources). These datasets may be available via downloads from the web via click through licenses.

8. These standards do not cover access to sensitive or personal data, or data that requires any kind of contractual guarantee from the LSE or RLAB. Access to these data types is covered in the document *RLAB Security Standards for Sensitive Data.*

9. These standards do not cover primary data resources created by researchers.

Definitions

10. Data contract/license refers to a formal agreement entered into by a member of the RLAB in return for access to research data. As outlined above, this includes (but is not restricted to) click through licenses as well as agreements that must be signed in hard copy.

11. Data Resources refers to all IT and contractual resources provided to researchers to store, safeguard, and analyse their data, as well as the data themselves.

12. Members refers to all staff, students, associates, visitors and others working with RLAB resources.

13. RLAB domain refers to dedicated subnets of the LSE IT network on which RLAB servers, PCs, and users are managed. This enables RLAB IT staff to have increased control over IT security than would be possible as part of the LSE domain.

Standards

14. Access to the RLAB IT facilities is only available to registered RLAB members via user specific, password protected accounts controlled by the IT Manager. These accounts abide by the *LSE Password Policy* which enforces high complexity and length of 15 or more characters.

15. In order to register as a data user and access the RLAB network, all staff, students, associates and visitors must complete the *RLAB Data Security Agreement* prior to accessing or storing any data within the RLAB domain.

16. Data that are contractually restricted to specific programmes, projects, or individuals will be accessed only by members covered by the contract.

17. RLAB members must not copy or pass data to any unlicensed person.

18. Visitors to the RLAB may be able to access data resources depending on the conditions of their data license and following consultation with a centre manager.

19. Researchers from other institutions who do not have employment/associate /visitor status with RLAB cannot access any RLAB IT/data resources even if they are involved in a collaborative project with RLAB members.

20. On leaving the RLAB members may only remove data that is licensed to them at an individual level.

21. The RLAB conforms to the *Conditions of Use of IT Facilities at the LSE*, the *LSE Information Security Policy* and the *LSE Information Classification Standard.*

22. All devices used to access or work on data conform to the *LSE Minimum Standards for device security.*

Licensing

23. RLAB members are responsible for ensuring that they hold valid, up to date licenses for all data resources they are accessing.

24. RLAB members will at all times abide by any license or contractual conditions associated with their access and analysis of research data.

25. Members must be aware at all times that data licenses are legal documents and any breach of the terms of the document may lead to sanctions being taken, by both the LSE and the data provider.

Storage

26. As standard all data resources should be stored on secure networked spaces (J: for CEP and SERC, Z: for STICERD and CASE) or on the RLAB remote desktop servers.

27. Data should only be stored on a member's PC hard drive for analysis purposes, and only where such local storage does not compromise data security. Data should be removed to a network drive as soon as the analysis is complete.

28. It is recommended that to reduce the risk of data loss no data should be stored on portable storage (e.g., USB hard drives or memory sticks). Where there is genuine need to store data on a portable device, members should consider using a drive that has either software or hardware encryption**.** It is advisable to store these devices in a secure location e.g., in locked desk drawer.

Security

29. Access to the RLAB is via swipe card only and is restricted to members.

30. All offices have locks, and the IT offices have additional swipe card locks which are only accessible by the RLAB IT team.

31. All RLAB servers are located in a secure server room. The server room is accessed via two locked doors within the swipe card restricted area. Keys are held only by the IT team and centre managers.

32. All data are stored within password protected folders that can be accessed only by licensed users (and IT staff)

33. PCs have a screen lock implemented automatically after 7 minutes. This lock can only be disabled by the active user (or a member of the IT team).

34. All computer hard drives that have held data are removed and degaussed using a National Cyber Security Centre approved device, http://www.veritysystems.com/products/sv91m/, before being sent to a certified recycling agent.

35. Access permissions for user network spaces are removed on the member leaving the RLAB.

Roles and Responsibilities

36. Members of the RLAB are responsible for adhering to any license/contractual conditions associated with their data access.

37. Any data contract which requires an institutional guarantee must be lodged with the centre manager and signed by the Director of the LSE Research Division. Any data contracts signed by other members of staff (e.g., heads of department, PhD

supervisors, project principal investigators) on behalf of the LSE/RLAB will not be legally valid.

38. The centre managers will provide support for data purchase, and contractual and licensing issues.

39. Data support, including advice on data resources available within the LSE, will be provided by the LSE Library (datalibrary@lse.ac.uk).

40. All ONS Accredited Researchers MUST take the following precautions during any remote access from home to ONS data held on the SRS or SDS system during the Corona Pandemic
    a. They must only work from their agreed nominated UK address,
    b. They MUST inform the SRS Research Support team if they access the SRS from a place that is not their home address i.e., an agreed secure room or Government site such as the Bank of England.
    c. They MUST NOT leave the computer unattended or on show, i.e., in a conservatory.
    d. Accredited Researchers MUST sign off or disconnect from the SRS environment and Remote Access Sessions as soon as they have completed their remote access requirements (this includes taking short breaks etc). Laptops must be shut down completely once work has been concluded.
    e. Access is only through a machine and connection provided by the researcher's organisation. No use of personal computers is allowed.
    f. Access is only allowed where a researcher already has remote access from their organisation approved by ONS under the Assured Organisational Connectivity scheme.
    g. No remote access will be allowed outside normal working hours, without prior written agreement with ONS.
    h. Approval will be on a project-by-project basis for individual researchers.
    i. Approval to access data to work on a specific research project will not mean that access for any other research project has been approved.
    j. Take reasonable precautions to ensure that other household members do not see the laptop screen.

Reporting

41. Any actual or suspected breach of data security must be immediately reported to the Centre Manager who will take appropriate action and inform relevant authorities.

Disciplinary procedures

42. Failure to comply with these standards or its subsidiary regulations may result in disciplinary action in accordance with procedures outlined in the *Conditions of Use of IT Facilities at the LSE.* Disciplinary action may include loss of RLAB Membership and access to RLAB facilities. Non-compliance with data access contracts may also

lead to data providers imposing sanctions including criminal charges and loss of ESRC funding.

Reference documents

43. RLAB Sensitive Data Security Standard
    https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Security_Standards_for_Sensitive_Data.pdf
44. RLAB Data Security Standard: Secondary Data
    https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Data_Security_Standards.pdf
45. RLAB Data Security Agreement
    https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Data_Agreement.pdf
46. RLAB Remote Working Guidelines
    https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Remote_Working_guidelines.pdf
47. Conditions of Use of IT Facilities at the LSE
    https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/conOfUseOfITFacAtLSE.pdf
48. LSE Information Security Policy
    https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecPol.pdf
49. LSE IT Services Password Policy
    https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/internal/staffAndStudents/pasPol.pdf
50. LSE Information Classification Standard
    https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecStaIT.pdf
51. LSE Minimum Standards for device security
    https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/internal/staffAndStudents/devLevSecMin.pdf

Key Contacts	
Harriet Ogborn Centres Manager (CEP, CVER, What Works Centres)	02079557285 H.Ogborn@lse.ac.uk
Marta Wasik STICERD and CASE Manager	02079556679 M.M.Wasik@lse.ac.uk
Nic Warner RLAB Information Technology Manager	02079557432 n.s.warner@lse.ac.uk
Jen Fensome Director, LSE Research and Innovation	02079557114 J.Fensome@lse.ac.uk
Hannah Boroudjou LSE Library Research Data Librarian	Datalibrary@lse.ac.uk
Muslim Saadat LSE Information Security Manager	02034862802 M.Saadat1@lse.ac.uk
Rachael Maguire LSE Records Manager (advice on DPA etc)	02079554622 r.e.maguire@lse.ac.uk
Hitesh Patel Information Systems & Data Administrator	02079557740 H.Patel12@lse.ac.uk

Document Control

Access Limitations:	None
Creator	Tanvi Desai, RLAB Data Manager
Maintainer:	Nicholas Warner, RLAB IT Manager Harriet Ogborn, Centres Manager (CEP, CVER, What Works Centres) Hitesh Patel, Information Systems & Data Administrator
Replaces	RLAB Data Security Policy
Review period:	This document is reviewed every 12 months. If no changes are required a new version is not released.
Is related to:	RLAB Research Data Security Policy RLAB Sensitive Data Security Standards RLAB Data Security Agreement RLAB Remote Working Guidelines Procedures for Accessing the RLAB Secure Server Conditions of Use of LSE IT facilities LSE Information Security Policy LSE IT Services Password Policy LSE Information Classification Standard LSE Minimum Standards for device security

Version History

Version	Notes	Last Amended
1.00	Drafted by Tanvi Desai	02/07/2012
1.00	Passed to Nic Warner and Nigel Rogers for comment	02/07/2012
1.01	Redrafted by Tanvi Desai	20/09/2012
1.01	Finalised by Tanvi Desai	28/09/2012
1.01	Responsibility for maintaining document handed to Nigel Rogers	28/09/2012
1.02	Updated by Nicholas Warner	21/09/2016
1.03	Updated by Nigel Rogers	04/11/2016
1.04	Finalised by Nic Warner	10/02/2017
1.05	Updated by Nic Warner	29/10/2018
1.06	Updated by Nic Warner	15/03/2019
1.07	Updated by Nic Warner	21/04/2020
1.08	Updated by NW to include requirements for home access to SRS/SDS systems	22/01/2021
1.09	Updated by NW to add in new LSE password policy details	25/11/2021
1.10	Updated by Hitesh Patel	08/07/2022
1.11	Updated by Hitesh Patel	13/10/2022
1.12	Updated by Hitesh Patel	20/06/2023
1.13	Hitesh Patel – updated LSE password policy URL, LSE Information Security Officer	12/06/2024