LSE Research Laboratory Security Standards for Sensitive Data

Description: The London School of Economics Research Laboratory standards for access and use of sensitive secondary data (including personal 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 safe storage and use of sensitive and personal 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 who are accessing sensitive or personal data under contract, 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, CEP, CVER, STICERD, What Works Centre for Wellbeing, What Works Centre for Local Economic Growth.

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 footage, computer files etc).

7. These standards are in addition to those outlined in the *RLAB Data Security Standard*, and for sensitive data both documents must be implemented together.

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

Definitions

9. Sensitive or personal data, consist of detailed data that contain information on individuals (including households or firms) that could potentially be used to identify those individuals, or allow information that would not otherwise be in the public domain to be associated with them. These datasets are usually made available under strict licenses that have conditions for the storage, use and disposal of the resource.

10. Personal data is a legal term. A formal definition can be found here https://ico.org.uk/media/1549/determining_what_is_personal_data_quick_reference_guide.pdf

11. Data contract/license refers to a formal agreement entered into by a member of the RLAB in return for access to research data.

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

13. RLAB domain refers to a dedicated subnets of the LSE IT network on which all RLAB servers, PCs, and users are managed.

14. Remote access to external providers refers to systems that provide a remote connection to a data provider allowing users to either access or execute

programs on the sensitive data remotely (remote access and remote execution).

Standards

15. A secure server is available within the RLAB for members needing to store, access or analyse sensitive data.

16. Access to the Secure Server is restricted to members who have signed an *RLAB Data Security Agreement* and who have satisfied a centre manager that they have the appropriate licenses to support access to the data. The Centre Manager will then authorise the IT Manager to arrange passworded access to a secure data folder containing the confidential data for the RLAB Member.

17. Where the standard secure server solution does not meet with a data provider's security requirements the RLAB will offer an alternative solution dependent on institutional and budgetary constraints.

18. On leaving the RLAB members may not remove any data that is accessed via an institutional license. Data (other than final outputs for publication) should only be removed from the Secure Server with the permission of a centre manager.

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

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

Licensing

21. Any contract requiring an institutional guarantee must be signed by a member of staff with the legal status to represent the LSE (for example the Director of the Research Division, see responsible staff below).

22. Members should be aware that all data classified as 'personal' are covered by the Data Protection Act (DPA). In general, a contract will specify whether data is 'personal data' but in case of any doubt the DPA should be applied.

23. For all data stored on an RLAB secure data server all documents regarding the contract and any email correspondence between the data provider and the

project leader will be stored centrally for administration and auditing purposes. No access will be given to the project data until this documentation has been passed to either the Centre Manager or the RLAB IT Manager.

Storage

24. For sensitive data resources stored on the Secure Server, only syntax and final outputs for publication should be removed from the Secure Server.

25. Sensitive data should not be stored on an external drive or removable device (e.g. CDRom, USB etc.). Where data is supplied on a removable device, members must ensure that the device is secured at all times before passing to the IT Manager for uploading to the secure server. Where necessary the RLAB IT Manager may grant permission for devices to be stored within the IT fire safe in the secure server room.

26. Data stored in the fire safe will be audited at regular intervals by IT staff. Data will be destroyed according to contractual requirements and in cases where a member of staff does not respond to email queries regarding the status of the data.

27. To comply with the Data Protection Act members should store the minimum number of copies of personal data. Ideally one raw file, and one working file. Members should store the programs that enable the files to be recreated from raw files.

Secure Server

28. Data on the secure server are stored within password protected folders that can be accessed only by licensed users (and IT staff). These folders are assigned by project and access granted according to licensing conditions on approval by a centre manager.

29. At the end of a data contract, the folder(s) containing the contract data and any other derived files are deleted from the server. At the end of the hardware's usable life all storage drives that have held the data are removed and degaussed using a National Cyber Security Centre approved device, http://www.veritysystems.com/products/sv91m/, before being sent for disposal.

30. Only the IT Manager can upload software to the Server. Software installation will only be approved following testing to ensure that it does not compromise server security.

31. There is no access to the internet from the Secure Server.

32. There is no facility to copy or paste data from the remote server window to a client computer.

33. An automatic screen saver is implemented on the Secure Server that locks the screen after 7 minutes of inactivity (standard on RLAB machines is 12 minutes).

34. Files from the Secure Server cannot be downloaded to USB sticks or other removable devices. Files from the Server can only be moved to a secure RLAB network drive for which the user has password access, except in cases where copying of data has been forbidden by the terms and conditions in the data providers' licence. In this case, this facility will be blocked.

35. Data, other than outputs for final publication, may under no circumstances be removed from the secure server.

Remote access to external providers

36. Any member accessing sensitive data via a secure remote connection to the data provider (e.g. Secure Data Service) must inform the RLAB manager, and provide a copy of their institutional and individual contracts.

37. Any member using a secure remote connection must ensure that they comply with all physical security conditions of their contract e.g. that their screen is not easily overlooked. If this is not possible they must apply to the manager of their Centre for a desk move in advance of accessing the secure connection.

38. Any member remoting into the RLAB server must ensure compliance with 36 above and sign their agreement to the conditions in the RLAB remote working regulations document.

39. No screen sharing software is installed on any machine with external remote access to sensitive data.

Roles and Responsibilities

40. RLAB members are expected at all times to understand and abide by conditions associated with their data access. Members must ensure that all efforts are made to safeguard their data sources, and that their actions do not have a negative impact on the reputation of themselves, LSE or the RLAB.

41. In cases where data access requires an institutional guarantee, members are responsible for notifying a centre manager and the institutional representative of clauses in their contract that might impact the institution.

42. The Director of the LSE Research Division is responsible for institutional contracts. 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.

43. In addition to requiring secure data users to sign up to the responsibilities outlined in the *RLAB Data Security Standard,* centre managers will verify that the security measures in place meet contractual requirements before authorising access to the Secure Server.

44. The IT Manager will provide secure solutions for managing storing and analysing sensitive data resources. The IT manager is not responsible for ensuring that the solution meets contractual requirements. That is the responsibility of the RLAB member.

Reporting

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

Disciplinary procedures

46. Failure to comply with these standards or their 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

47. RLAB Sensitive Data Security Standard
    https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Security_Standards_for_Sensitive_Data.pdf
48. RLAB Data Security Standard
    https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Data_Security_Standards.pdf
49. RLAB Data Security Agreement
    https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Data_Agreement.pdf
50. RLAB Remote Working Guidelines
    https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Remote_Working_guidelines.pdf
51. Conditions of Use of IT Facilities at the LSE
    https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/conOfUseOfITFacAtLSE.pdf
52. LSE Information Security Policy
    https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecPol.pdf
53. LSE IT Services Password Policy
    https://info.lse.ac.uk/staff/divisions/dts/password/LSE-password-policy
54. LSE Information Classification Standard
    https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecStaIT.pdf
55. LSE Minimum Standards for device security
    https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/internal/staffAndStudents/devLevSecMin.pdf
56. Data Protection Act
    https://www.legislation.gov.uk/ukpga/2018/12/contents

Key Contacts

Harriet Ogborn Centres Manager (CEP, CVER, What Works Centres)	02079557285 H.Ogborn@lse.ac.uk
Annie-Rose Nicholas STICERD and CASE Manager	02079556679 A.Nicholas1@lse.ac.uk
Nic Warner RLAB Information Technology Manager	02079557432 n.s.warner@lse.ac.uk
David Coombe Director, LSE Research and Innovation	02079557114 d.coombe@lse.ac.uk
Helen Porter LSE Library Research Data Librarian	02079557238 Datalibrary@lse.ac.uk
Jia Fu LSE Information Security Manager	02034862802 J.Fu8@lse.ac.uk
Rachael Maguire LSE Records Manager (advice on DPA etc)	02079554622 r.e.maguire@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)
Replaces	RLAB Sensitive 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 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	04/07/2012
1.00	Passed to Nic Warner and Nigel Rogers for comment	04/07/2012
1.00	Amended by Tanvi Desai following comments from NW/NR	05/07/2012
1.01	Version finalised by Tanvi Desai	28/09/2012
1.01	Responsibility for maintaining document handed to NR	28/09/2012
1.02	Updated by Nicholas Warner	21/09/2016
1.03	Amended by N.Rogers following discussion with N.Warner	04/11/2016
1.04	Finalised on discussion between NR and NW	10/02/2017
1.05	Updated Nic Warner	29/10/2018
1.06	Updated Nic Warner	15/03/2019
1.07	Updated Nic Warner	21/04/2020
1.08	Updated by NW to include new DPA 2018	22/01/2021

1.09	Updated by NW to include the new LSe password policy	25/11/2021