RLAB Data Security Information

London School of Economics & Political Science
Sir Arthur Lewis Building, 32 Lincoln's Inn Fields, WC2A 3PH

Summary information for data providers

The LSE Research Laboratory (RLAB) and its member centres[1] have over 25 years of experience in managing large national and international survey and administrative datasets many of which require secure storage because of their confidentiality. Our assurance of best practice to data providers that we store, retrieve, and give access to data in a secure environment, and that we ensure data is used in line with specific data provider regulations is based on six factors summarised below and then more fully documented:

1. Our research centre is in a separate building – Sir Arthur Lewis Building, 32 Lincolns Inn Fields, London WC2A 3PH access to which is through a manned reception for staff and students with the necessary LSE entry cards. Doors in corridors are locked down out of working hours and are only accessible with the use of such entry cards.
2. We have a dedicated IT Manager responsible for the storage, security, backup, provision of access to and destruction after use of datasets including detailed data on education, employment, tax, firms, trade, health etc. and a Centre Manager supported by an information administrator responsible for all data and personnel contractual arrangements and records.
3. We have the technical infrastructure to store the data on secure servers locked in a secure room with double password authenticated access provided by the IT Manager to those researchers who have documented authorisation to use the data.
4. We have the necessary administrative and regulatory infrastructure to manage contractual compliance with data providers and monitoring of each project's storage of data, use and final disposal of data. All researchers using data are required to confirm their adherence to the conditions of receiving data from data providers, and to comply with the Centres' regulations. The Centres are all departments of the London School of Economics, and their regulations are backed up by the LSE's information security regulations https://info.lse.ac.uk/staff/divisions/dts/about/policies.
   Contravention of either can lead to the School's disciplinary procedures being invoked.
5. No employee, associate student or visitor of the Centres is permitted to keep or make a "local" copy of licensed data on their pc, laptop, digital storage devices or media: access can only be through the secure server by use of dual password authentication provided by the IT Manager. The access can be monitored. Only authorised personnel with LSE entry cards and an LSE key fob (Salto) can gain access to their office and PC. Each PC has an automatic lockdown of its screen after a short interval of non-use, re-openable only by password. Where data provider conditions require it, we can restrict any downloading of data and/or calculations to the secure server alone, researchers thus only being able to work on the data remotely.

[1] including the Centre for Economic Performance (CEP), the Centre for Vocational Education Research, the Spatial Economics Research Centre, the What Works Centre for Local Economic Growth, Suntory Toyota Centre for Economics & Related Disciplines, Centre for the Analysis of Social Exclusion

6. Other national data agencies in the UK and overseas have approved our data infrastructure and given their data for storage and access: they include the Secure Data Service https://www.ukdataservice.ac.uk, including access through their SDS remote access system, Hospital Episode Statistics of the National Health Service https://digital.nhs.uk/data-and-information/data-tools-and-services/data-services/hospital-episode-statistics; National Pupil Database of the Department for Education https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract; Census Data through IPUMS https://usa.ipums.org/usa/full_count.shtml ; the Research Data Centre of the German Federal Employment Agency; https://fdz.iab.de/en/startseite-en/; several government departments have jointly authorised the use and matching of administrative and survey data via the Research Lab's data infrastructure.

We now turn to the details of the LSE RLAB's security policies and technical infrastructure.

Information Security Policy

All people using sensitive data on the RLAB systems have to conform to the following policies; The Research Laboratory Sensitive Data Security Standard, the RLAB Data Security Standard; the Conditions of Use of IT Facilities at LSE.

https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Data_Security_Standards.pdf
https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Security_Standards_for_Sensitive_Data.pdf
https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/conOfUseOfITFacAtLSE.pdf

All staff in the research centres using confidential data are required to sign the RLAB Data Agreement before gaining access to passworded folders on the data servers, which are centrally controlled by the Information Technology Manager, Nic Warner.
https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Data_Agreement.pdf
All data licensees are required to provide the centre/department managers with all licensing documentation before authorisation is given to the IT Manager to allow access to the data. Copies of the licence documentation are kept centrally by the centre/department managers and the IT Manager. Licence expiry dates are logged in a central system maintained by the RLAB IT Manager and access to data withdrawn on expiry. The centre/department managers and IT Manager report to and advise the Directors of the RLAB, Professor Stephen Machin and Professor Camille Landais, on all aspects of data security and management. The RLAB data security documents are continually revised to reflect new procedures, technological developments, and data provider requirements and are submitted to the Directors for approval.

The documents above refer to internal departmental data security procedures. However, the RLAB is a department within the London School of Economics and staff in it are required to sign up to the LSE's 'Conditions of Use of IT Facilities' also. By accessing and/or using the IT Facilities at LSE, all staff are bound by these Conditions of Use and all documents referred to

in it. Their attention is particularly drawn to the section on working practices and the penalties including expulsion/dismissal from the School for breach of these Conditions. The School requires that all data owned, processed or held by LSE, whether primary or secondary, must be accessed, stored, processed and backed up in a manner appropriate to its security classification. LSE's data classification guidelines can be found at https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecStaIT.pdf.
Failure to appropriately classify and handle data is a breach of these terms and conditions.

Anyone accessing the server from outside the LSE will be working with the remote working guidelines contained here https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Remote_Working_guidelines.pdf.
Requests for remote access from abroad for staff carrying out research visits travelling out of the UK will be made to data providers if their license requires it.

All contracts with data providers are signed by the Director of the Research Division, Jen Fensome.

ISO27001

Whilst the LSE is not certified to ISO27001 it is using the ISO27000 family of standards to inform our approach on information security.

LSE Information Security Policies embed the principles found in the ISO27002 best practice controls, and lay out rigorous standards around 'least privilege' and 'need to know' for the operation of all systems.

The LSE Information Security Policy, accompanying policies, and the Information Security Classification Standard documents can be found here:

https://info.lse.ac.uk/staff/divisions/dts/about/policies

The appropriate RLAB policies governing use of the data are referenced in the previous section.

Risk Assessment & Audit

The LSE Information Security Advisory Board develops all IT security policies, https://info.lse.ac.uk/staff/divisions/dts/about/policies, chaired by the LSE Director of Governance, Legal and Planning Division.

All IT security policies are taken to the Information Governance Management Board, which is chaired by the School Secretary.

The LSE IT Infrastructure is penetration tested annually by external contractors, and any service found to be vulnerable is remediated. The last security penetration test was carried out in May 2020, with further tests scheduled for October 2021. They are conducted annually

by an external contractor for LSE Data and Technology Services Division (DTS) across a selection of critical IT systems including those used in RLAB for analysing data provided by the DfE.

LSE DTS run annual internal audits (performed by external contractors) on elements of information security. The last audit of one of our systems took place in August 2020. Actions in response to the findings are completed and the best practice recommendations are being applied to all our systems.

Operational IT risks at LSE are recorded and managed via the IT Operational Risk Committee.

Controls over users are carried out by the centre/department managers who vet applications to Data Providers, checking with centre/programme directors that projects for which data are sought have officially been agreed as part of the Centre's research programme and that the project for which data is requested does not extend beyond the employment contract end date; the centre/department managers check authorisation is given by data providers before allowing the encrypted data from the Department to be uploaded by the IT Manager to the secure server. Access to the data on the server is terminated at the end of a project or automatically at the end of the data user's LSE contract, whichever is sooner. The RLAB is audit-ready and keeps a listing of holdings, and owners, permissions, project dates and full licensing application and permissions documentation.

System details

The data is stored on a server that resides on a corporate IT network, inside a firewall, it is password protected and has limited access to network storage. The machine is remotely accessible via another password system through a VPN. Nothing can be copied to or from the system via the remote connection.

The server operates on a minimum of Microsoft Server 2016 and is manually patched regularly. It runs the Anti-virus software Trend that is updated automatically, this also runs an anti-malware and application protection service that secures and restricts the applications running on the server. The server has all web access blocked by Active Directory policies.

Remote access to the server is provided using Microsoft's Remote Desktop Client. The ability to use copy and paste, printing, and internet access on this server is blocked at a system level. External access is provided via the Pulse Secure SSL VPN gateway, requiring perimeter authentication against valid user accounts, and providing a secure encrypted VPN between endpoints and the RLAB Server.

The LSE run Juniper SRX5400 firewalls with default deny inbound policies. The network switches on campus are Cisco.

Access Policy

Once encrypted data is passed to the Research Lab it only ever resides on a secure server and individuals obtain access to the folder in which the data reside through a unique passworded account. Access is only provided to the specified Active Directory accounts for those people

listed on the data contract. This is allocated by the IT Manager on the authorisation of the centre/department managers, following placement of all data licences and authorising data provider documentation on the data server. RLAB policies and the security setup of the server do not allow transferring of data to portable hard disk, USB storage or other removable media; a Research Lab member's working files from the server can only be moved to a secure RLAB network drive for which the person has passworded access. This and the signing of the RLAB data security documents ensures staff conform with the terms and conditions of providers forbidding the copying of sensitive/confidential data.

Physical Security

The server resides in a locked cage inside a locked dedicated secure air-conditioned data room inside the IT Managers room accessible by swipe card coded for IT staff only; the IT room is in the Research Centre on the 3rd floor of Sir Arthur Lewis Building, 32 Lincolns Inn Fields WC2, access to which is via 24/7 security manned reception and swipe card turnstile entry.
The data only ever resides on the secure server within the above secure location, which is only accessible by the RLAB IT Team, so any means of removing the data via a physical data storage method is not possible.

Data destruction

At the end of a data contract, the folder(s) containing the contract data and any other derived files are deleted from the server. This can be done using standard Windows operations or using specialist software like Eraser, https://eraser.heidi.ie/, which will securely remove the data using overwriting techniques. Then 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.

Extended Technical details

The raw data will reside on an iSCSI volume connected to the server; this volume is from a Dell Compellent iSCSI SAN containing sixteen 3TB drives running Raid 6. This SAN is located in a secure dedicated server room within the Sir Arthur Lewis Building. This volume is backed up to a second SAN, based at the LSE's secure data centre in Slough, once every three days and a maximum of four backups are kept before being over written. This SAN will come under the same destruction policy as the one holding the data, as mentioned above.

Any derived data will be on a dedicated hard drive that resides in the server which can have the Microsoft BitLocker encryption enabled, this drive will not be backed up.

The user account accessing the server has an expiry date that disables the account once reached. There is a password policy that requires the password to be a minimum length of 15 characters and requires a high level of complexity and should include upper- and lower-case letters, numbers and symbols.

Reference documents

1. RLAB Sensitive Data Security Standard
   https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Security_Standards_for_Sensitive_Data.pdf
2. RLAB Data Security Standard
   https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Data_Security_Standards.pdf
3. RLAB Data Security Agreement
   https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Data_Agreement.pdf
4. RLAB Remote Working Guidelines
   https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Remote_Working_guidelines.pdf
5. Conditions of Use of IT Facilities at the LSE
   https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/conOfUseOfITFacAtLSE.pdf
6. LSE Information Security Policy
   https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecPol.pdf
7. LSE IT Services Password Policy
   https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/internal/staffAndStudents/pasPol.pdf
8. LSE Information Classification Standard
   https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecStaIT.pdf
9. LSE Minimum Standards for device security
   https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/internal/staffAndStudents/devLevSecMin.pdf
10. 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
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 Division	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)	0207955s4622 r.e.maguire@lse.ac.uk
Hitesh Patel Information Systems & Data Administrator	02079557740 H.Patel12@lse.ac.uk

Document Control

Access Limitations:	None
Creator	Nicholas Warner, RLAB IT Manager
Maintainer:	Nicholas Warner, RLAB IT Manager Harriet Ogborn, Centres Manager (CEP, CVER, What Works Centres) Hitesh Patel, Information Systems & Data Administrator
Replaces	Information Security Questionnaire
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 Sensitive 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 Nic Warner	12/01/2018
1.00	Passed to Nigel Rogers for comments	20/02/2018
1.00	Amended by Nic Warner following comments	28/03/2018
1.01	Version finalised by Nic Warner	28/03/2018
1.02	Updated to include new web links by Nic Warner	30/10/2018
1.02	Restructured by Harriet Ogborn	19/02/2019
1.04	Finalised on discussion between Nic warner and Harriet Ogborn	01/03/2019
1.05	Added information about new penetration testing, server 2008 R2 end of support and IMT rebranding as DTS	20/06/2019
1.06	Updated by Nic Warner	21/04/2020
1.07	Updated by NW to include new DPA 2018	22/01/2021
1.08	Updated section on Risk Assessment and Audit - NW	12/08/2021
1.09	Updated to include the new LSE password policy - NW	25/11/2021
1.10	Updated section on Risk Assessment and Audit - NW	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 NHS/HES link	12/02/2024
1.14	Updated by Kalliopi Vacharopoulou (edits to National Pupil Database Link and Harriet Ogborn’s position)	28/10/2024