LSE Research Laboratory Guidelines for Remote Working when accessing Sensitive Data

Description: The London School of Economics Research Laboratory (RLAB) guidelines for Remote Location Working on sensitive data held on RLAB remote access servers

Introduction

The availability of sensitive secondary data resources underpins the work of the LSE RLAB research programmes. Therefore, the security, confidentiality and good management of data resources are key to the success of the RLAB and to retaining the confidence in our systems of secure data providers. Failure to secure data access increases the risk of legal sanctions and reputational loss from which it may be difficult to recover.

Purpose

This document outlines LSE RLAB guidelines for users accessing sensitive data stored on RLAB remote access servers from outside the LSE.

Scope

These standards are applicable to, and will be communicated to, all members of the RLAB using sensitive data on RLAB remote access servers.

For the purposes of this document the RLAB includes the following research centres: CASE, CEP, CVER, WHAT WORKS CENTRES (Local Economic Growth and Wellbeing) and STICERD.

This document is relevant to users of both LSE owned and personal laptop and desktop computers (though LSE-owned equipment is the preferred option from maintenance, compatibility and virus protection standpoints.)

Guidelines

1. You may only connect to the server by using the LSE or RLAB VPN: for installation see https://rlab.lse.ac.uk/itsupport/GUIDES/connect-to-RLAB-IT-resources.asp

2. You may only access the server from a private location, not from public areas, for example coffee shops, or airports.

3. You may only use known secure private network connections, not free networks, which are easily snooped upon, generally found in airports and hotels and an increasing number of public places.

4. You must ensure your computer has an automatic screen lock turned on, so that if the device is left for a short period of time the machine will lock and require a password to gain access. We recommend a maximum time limit of five minutes until it locks.

5. You must ensure the password you use meets LSE's length and complexity rules (https://info.lse.ac.uk/staff/divisions/dts/password/LSE-password-policy)

6. If your remote computer is shared with anyone else it must have a different account set-up to the one you use to access the RLAB server.

7. Do not cache any credentials you use to access the server, either in the VPN client or in the remote access software. This will require you to enter your RLAB password to connect each time you want to access the server.

8. Any device accessing the server must be fully updated and running an updated version of the LSE anti-virus software Sophos.

9. Any device accessing the server must be fully patched and regularly kept up to date – both the Operating System and all applications

10. Any integrated firewall product contained in the Operating System (e.g. Windows or Mac) must be switched on.

11. If you are outside the United Kingdom make sure you have written confirmation from the data provider that you are allowed to access the sensitive data server. A lot of providers restrict this.

12. If you are using a computer based at another institution or work place, when you leave please make sure the IT team delete your profile on the machines you have used to access the data server, or if possible request the machine to be wiped.

13. We recommend that the hard drive on the machine from which you are remotely accessing the server is encrypted. This is now easy to do both on Microsoft Windows and Apple OS X and has very little impact on the performance of the computer. For help with setting this up please see the IT team.

14. No copy of the data will be removed from the RLAB Servers.

15. The research team has completed the mandatory Moodle data security training (you can self-enrol at https://moodle.lse.ac.uk/course/view.php?id=6416).

16. 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 laptop unattended or on show, i.e. in a conservatory.
    d. ARs 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

17. Any actual or suspected breach of data security must be immediately reported to the Centre Manager and RLAB IT Manager who will take appropriate action and inform relevant authorities. Any suspected unauthorised data exposure or breach over the usage of their data, will be reported to dts.cyber.security.and.risk@lse.ac.uk in the first instance and if necessary escalated to the Information Commissioner's Office (ICO) if required by the contract or LSE policy.

Support

18. For help with setting your computer up using these guidelines please see the RLAB IT team or the help resources on the RLAB-IT website. See below for a summary of the minimum requirements for setting up your remote computer:

    - Full drive encryption applied (e.g. FileVault on Mac, BitLocker for Windows, VeraCrypt for Windows Home Edition).
    - The encryption key should be at least:

        - 15 characters long
        - Contain at least one upper case letter and at least one lower case letter
        - Contain at least one number or punctuation character
        - Avoid international (non ASCII) characters
        - Not be a dictionary word
    - You have a strong password for your device, using the same complexity as above
    - Have an anti-virus software installed and will run regular scans
    - Actively operate a software firewall (enable the built-in firewall option in the operating system)
    - Keep the operating systems up to date by installing security patches as soon as they are released
    - Keep other software up to date by implementing security patches as soon as they are released
    - Apply a screen saver that automatically locks after 5 minutes inactivity

Reference documents

- RLAB Sensitive Data Security Standard
  https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Security_Standards_for_Sensitive_Data.pdf
- RLAB Data Security Standard
  https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Data_Security_Standards.pdf
- RLAB Data Security Agreement
  https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Data_Agreement.pdf
- RLAB Remote Working Guidelines
  https://rlab.lse.ac.uk/itsupport/downloads/files/LSE_Research_Laboratory_Remote_Working_guidelines.pdf
- Conditions of Use of IT Facilities at the LSE
  https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/conOfUseOfITFacAtLSE.pdf
- LSE Information Security Policy
  https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecPol.pdf
- LSE IT Services Password Policy
  https://info.lse.ac.uk/staff/divisions/dts/password/LSE-password-policy
- LSE Information Classification Standard
  https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecStaIT.pdf
- 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
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	Nicholas Warner, RLAB IT Manager
Maintainer:	Nicholas Warner, RLAB IT Manager Harriet Ogborn, Centres Manager (CEP, CVER, What Works Centres)
Replaces	None
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 Nicholas Warner	30/09/2016
1.00	Passed to Jethro Perkins and Nigel Rogers for comment	30/09/2016
1.01	Redrafted and finalised by Nicholas Warner	10/02/2017
1.02	Updated by Nic Warner	29/10/2018
1.03	Updated by Nic Warner	15/03/2019
1.04	Updated by Nic Warner	21/04/2020
1.05	Updated by NW to include requirements for home access to SRS/SDS systems	22/01/2021
1.06	Updated by NW to include new LSE password policy	25/11/2021