Security and Usage Policy for SRS Secure Suites at the School of Economics (SoE_SRS_SUP)

Operational Owner:	Head of the School of Economics
Executive Owner:	School of Economics SRS Liaison Officer(s)
Effective date:	19/10/2021
Review date:	23/05/2025
SoE Secure Suites Location	Ground floor of the AD (Elizabeth Fry) Building – Rooms 45 AD 00 and 46 AD 00
Related documents:	Acceptable Use Policy (https://www.surrey.ac.uk/sites/default/files/2022-05/acceptable-use-policy.pdf), and related Policies.

Approval History

Version	Created/ Reviewed by	Reason for review	Approved by	Date
1.0	Giuseppe Moscelli	First draft of the Security and Usage Policy for SRS Secure Suites at the School of Economics (SoE_SRS_SUP)	Head of Department (Maurizio Zanardi) and SoE SRS Liaison Officers (Giuseppe Moscelli, Matthias Parey)	19/10/2021
1.2	Giuseppe Moscelli	Changes to the policy due to the introduction of MFA by SRS	Liaison Officers (Giuseppe Moscelli, Matthias Parey)	07/06/2023
1.3	Giuseppe Moscelli	Changes to the policy to exclude home VPN access to SRS from common areas	Liaison Officers (Giuseppe Moscelli, Matthias Parey)	29/04/2024

1 Introduction

1.1 Purpose

The Security and Usage Policy for SRS Secure Suites at the School of Economics (SoE_SRS_SUP) is intended to protect you as well as the University and its School of Economics, and to ensure the University of Surreys' and its School of Economics are not in breach of the security requested to handle research data accessed via the ONS SRS.

1.2 Scope

The rules in the Security and Usage Policy for SRS Secure Suites at the School of Economics (SoE_SRS_SUP) are mandatory for all ONS Accredited Researchers (AR) that have been approved to access ONS data via the SRS access at the School of Economics (SoE), either through Home Assured VPN or through the two Secure Suites available at the SoE.

1.3 Definitions

User(s) - all University staff and students, temporary staff, affiliates or visitors, that are ONS Accredited Researchers (AR) as approved by ONS.

University Systems – any hardware, software, data, network access, third party services or online services provided or arranged by the University of Surrey.

SoE Secure Suites – Secure Suites to access ONS data located at the ground floor of the AD (Elizabeth Fry) Building.

Assumed VPN – Secure VPN connection using the VPN software provided by the University IT services.

SRS Liaison Officers – SoE staff member(s) tasked with the role of gatekeeper(s) to the SoE SRS facilities and SRS Assured VPN Home Access.

SRS Booking Register (BR) – an online spreadsheet to book for SRS Secure Suites usage.

Severe Breach – any breach of this Policy or related University Policies that might endanger the present and future fruition of the access to the ONS SRS services by the SoE staff.

2 Policy Terms

2.1 Registration to SRS services at the SoE

2.1.1 The current/prospective User must notify the SoE SRS Liaison Officers about the AR credentials, including their AR ID number and the ID number of their SRS project(s).

2.1.2 The School Secretary will provide the User with a list of documents to read, review and sign. The signed documents will need to be emailed to the SoE SRS Liaison Officers, and in copy to the School Secretary.

2.2 Access to the SRS Secure Suites (SESUs)

2.2.1 The authorized User is granted access to the Secure Suites by receiving a copy of the keys to the safe box where the keys for the two Secure Suites are held.

2.2.2 The User must book in advance their planned access to any of the Secure Room at least 24 hours before their intended usage of the service.

2.2.3 The booking must be made by using the SRS Excel spreadsheet register (SRS Booking Register; BR) provided by the either School Secretary or by the SRS Liaison Officers.

2.2.4 The booking must record: the day of the planned access, the day of the booking, the name of the AR User, the planned starting and ending time to access the SESU, the effective starting and ending time when the access to the SESU has occurred.

2.2.5 Each booking in advance cannot exceed the total duration of 4 continuative hours over a single day.

2.2.6 On the calendar day of the booking, Users are allowed to use the Secure Room for longer

than 4 hours (e.g. the whole day) if no other User has already registered to use the service; in this instance, the User must book their extended stay in the Secure Suites as an additional, separate entry in the SRS Booking Register.

2.2.7 After logging off, and within 24 hours from the effective use of the SESU, the User must update the BR with the effective times of initial entry and final exit from the SESU. Failure to comply with this norm for three times will incur into a one week temporary ban from accessing the SESUs.

2.2.8 No food or beverage is allowed in the SESUs. Failure to comply with this term will incur a one month temporary ban from accessing the SESUs.

2.2.9 No other IT equipment, either personal or provided by the University, is allowed in the SESUs. The use of mobile phones is permitted in the SESUs only to allow for Multi-Factor Authentication procedures to login to either the University of Surrey IT network, in order to access the SRS, and/or the SRS IT network. Failure to comply with this term will incur a six month temporary ban from accessing the SESUs, with the possibility for the ban to become permanent.

2.2.10 The SESUs are used by the User for the only purpose of accessing ONS data via the SRS. The IT resources available within the SESUs must not be used for services that can be accessed or obtained through other University or personal resources. Failure to comply with this term will incur a two month temporary ban from accessing the SESUs, with the possibility for the ban to become permanent.

2.3 Access to the SRS via Assured VPN Home Access

2.3.1 The User must notify the SRS Liaison Officer(s) that they have been granted permission to access the SRS remotely via the University VPN. The notification must occur by email.

2.3.2 The User must always access the SRS: (a) via the University provided VPN software / link; and (b) using compulsorily a University-maintained laptop. Failure to comply with this term will incur a four month temporary ban from accessing the SESUs, with the possibility for the ban to become permanent.

2.3.3 The AR User commits to a safe and responsible use of their temporary VPN access to the SRS from home, in order to prevent and/or minimize the risks for the confidentiality of the data accessed.

2.3.4 The AR User commits to accessing the SRS and/or IDS environment only from home or the designated organization premises (i.e. office rooms), excluding access from common areas such as a staff restaurant, coffee lounge, conference venues, train wagon or airport lounges.

2.4 Reporting Incidents

The User must notify via email a suspected security breach and/or a SRS data leakage within 24 hours from the incident to the SRS Liaison Officer(s), the School Secretary and the Head of School. Failure to comply with this term will incur a six month temporary ban from accessing the SESUs, with the possibility for the ban to become permanent.

2.5 Policy enforcement and breach sanctioning

2.5.1 Violations of these above conduct rules will be liable of disciplinary actions by the University.

2.5.2 Breaches of conduct must be timely reported to the SRS Liaison Officers, who will administer proportionate sanctions to the User(s) in the first instance and/or report the violation(s) to the HoS in case of particular gravity. Should a breach of conduct be deemed a Severe Breach by the HoS, a trialing Panel will be formed, with a member named by the Head of the School to which the AR belongs, a member named by the Dean of the Faculty, a member named by the University Head of Information Security and a member named by the Faculty Head of Human Resources.

2.5.3 The trialing Panel will: meet within 14 days from the discovery of the violation; hear the AR; assess the circumstances of the said breach of conduct and their gravity; finally, decide: (a) whether to initiate disciplinary actions against the AR and (b) the severity of the said disciplinary actions, including the temporary suspension from the SRS services.

2.6 Review and Change Requests

The policy will be reviewed annually or as necessary.

SoE_SRS_SUP - User Declaration Form

(this form must be signed by the User and submitted via email to the SRS Liaison Officer(s) and to the Secretary of the School of Economics)

Hereby I certify that I have read and understood the terms of the Security and Usage Policy for SRS Secure Suites at the School of Economics (SoE_SRS_SUP).

PRINT name

SIGNED by

. . . . . .

Adherence to the content of this document and the documents cited, is obtained on

[print date] . . . . . .

Signed copy to be retained by Helen Dee, School of Economics Secretary

You will be personally liable if you contravene this consent.

V1.3 as at 29th April 2024