Secure Access and Usage Policy for the Trusted Research Environment at the School of Economics (SAUP_TRE_SoE)

Operational Owner:	Principal Investigator of RF1095 project - Dr. Giuseppe Moscelli
Executive Owner:	University of Surrey IT Services Liaison Officer(s) – Mr Peter Wright
Effective date:	07/06/2023
Review date:	31/09/2024
School of Economics Trusted Research Environment Location	University of Surrey campus
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, Peter Wright	First draft of the TRE Secure Access and Usage Policy	Giuseppe Moscelli, Peter Wright	07/06/2023

1 Introduction

1.1 Purpose

The Secure Access and Usage Policy for the School of Economics Trusted Research Environment (SAUP_TRE_SoE) is intended to specify requirements for individual researchers employed at the University of Surrey (UoS), its School of Economics (SoE), or formally acknowledged as visitors at either UoS or SoE, to securely access the TRE and to be authorized to use, alter, disclose or destroy data stored within the Trusted Research Environment (TRE).

1.2 Scope

The rules in the SAUP_TRE_SoE are mandatory for all Researchers (REs) that have been approved to access the School of Economics (SoE) Trusted Research Environment (TRE).

1.3 Definitions

User(s) - all University staff, PhD students, temporary staff, affiliates or visitors, that are Researchers (REs) approved to access the TRE by the Principal Investigator (PI) of the RF1095 project.

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

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

IT Services Officers (ITSO) – UoS staff member(s) tasked with the role of gatekeer(s) to access and maintain the TRE.

1.4 TRE technical description

1.4.1 Objective. The SoE TRE is made accessible exclusively via the university VMware Horizon virtual desktop infrastructure environment. Access is controlled and brokered via a secure portal, which requires 2-factor authentication. Once authenticated, the User is allocated compute resource where data can be accessed and manipulated. Finally, the data is stored on an encrypted file server.

1.4.2 Connectivity. The UoS utilizes a VMware Horizon (virtual desktop infrastructure) environment to grant access to virtual and physical resources on and off-site. This environment is used to broker connectivity for internal and external users that need to work on this project. Users connect to the TRE using the following method: a) Connect to the university VPN solution (GlobalProtect) via MFA and then the ‘securedesktops.surrey.ac.uk’ portal using the VMware Horizon client. b) Authenticate using their university credentials + an additional layer of 2-factor authentication. This additional authentication is handled via RSA hardware tokens the Users require to connect to the infrastructure. c) Once authenticated, users will be shown the available compute resource for this project and can select as required.

All resources for this project are ‘tagged’ (made available) exclusively via the securedesktops.surrey.ac.uk remote access portal. This means it is not possible for these resources to be accessible via the standard desktops.surrey.ac.uk portal that the majority of university users connect to. In addition, access to resources are strictly controlled via Active Directory security groups. Only approved Users are allowed to connect to the project’s resources, and only via the aforementioned secure portal. Both criterion of group membership and access via the secure portal are required to access the resource.

Once authenticated, a remote session is established between the server and the remote compute resource. This is available via two selectable display protocols, RDP and VMware BLAST. Both protocols are encrypted, with BLAST utilizing SSL between the server and endpoint and RDP using native encryption.

1.4.3 Compute. Access and manipulation of the data is carried out on four dedicated servers. The servers are configured as Remote Desktop Session hosts so that multiple project members will be able to work on the datasets concurrently.

1.4.4 Storage. Data is stored on a virtual file server which itself sits on encrypted VMware VSAN storage. This means no data is stored in an unencrypted state on any physical disks which make up the storage solution, eliminating the chance for any data to be recovered from the disk drives once they are physically disposed of.

1.4.5 Connectivity between the servers and file server occurs via SMB. Users are able to access and save data to/from the file server via drive mappings preconfigured on each server.

1.4.6 Local storage on the servers occurs only for running the operating system and software apps used, and not for storing data or results. As a precaution, all local disks on the servers are encrypted via Windows Bitlocker.

1.4.7 Networking. The compute and file servers for this project reside within a dedicated subnet where all inbound and outbound access is controlled via a Palo Alto virtual firewall. This prevents access from any other university subnets. Only resources related to this project exist inside this subnet, more specifically the file and compute servers only.

1.4.8 Firewall rules are implemented only for the ports/protocols required to allow connectivity between the secure servers and Horizon infrastructure components, as well as to the project members' remote access client.

1.4.9 Backup. All data is backed up from the file server to the UoS's backup solution, Commvault. Backups are performed on the following schedule: Full Backups: Monthly on Friday's at 10pm; Daily Differential: Every Night at 10pm. All backups are processed by the dedicated storage policy for sensitive stored data. This means that all backups are encrypted to ensure compliance.

2 Policy Terms

2.1 Registration and access the SoE TRE

2.1.1 The project PI provides written instructions via email to the ITSO about the identity of the new researchers to be granted access to the TRE as new Users, on a case by case basis, and the expected period during which access to the TRE should be maintained.

2.1.2 The ITSO provides the new and existing TRE Users with RSA hardware tokens and technical support for access to the TRE and safe usage of stored data through the installed software.

2.2 Usage of the data

2.2.1 Any authorized User is granted access to all data stored within the TRE, unless the PI instructs the ITSO to grant a User only partial access, i.e. access to a given folder or dataset.

2.2.2 The PI can instruct the ITSO to make available specified data folders only to a restricted group of Users.

2.3 Data alteration and erasure

2.3.1 Users cannot alter or erase the source data without the permission of the PI.

2.3.2 Data used for the analysis are partially extracted or copied in separate folders from the source files, and analyzed within the separate folders.

2.3.3 Users cannot erase the manipulated data and script files necessary for the project analyis without the permission of the PI.

2.3.4 The project PI arranges the erasure of data obtained through any form of Data Sharing Agreement (DSA) to occur safely, with the erasure process to be operated by the ITSO.

2.4 Reporting Incidents

The User must notify via email to both the PI and the ITSO about any suspected security breach, data leakage or hardware/software malfunctioning within 24 hours from the incident. Failure to comply with this term will incur a disciplinary action, to be agreed by the project PI, the ITSO, and the SoE Head of Department.

2.5 Review and Change Requests

The policy will be reviewed annually or as necessary.