STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Restricted

Title:	**TRE User Manual and Agreement**
Effective Date:	**04 Sep 2019**
Reference Number:	**SOP-03-02**
Version Number:	**1.9**
Owner:	**Information Security Manager,**
Review Date:	**05 Sep 2020**

Please familiarise yourself with this whole User Manual and Agreement, and refer to it as needed during your project.

TRE users can:

- Connect securely to the TRE from a specified computer location
- Use the software provided to view, analyse, and summarise their project's data in accordance with the study protocol
- Create new files
- Request export of research output or installation of additional software
- Contact the TRE support team by email with any questions or comments

TRE users must not:

- Use data for any purpose beyond the study protocol
- Take pictures of the screen of their TRE session
- Export files or write down anything from the screen without the notes being checked and approved for release by the TRE Support team
- Allow anyone else to see their screen who is not a TRE project member
- Store passwords insecurely, e.g. store key pair and passphrase in the same location or share passphrase with anyone else
- Share this document

Table of Contents

1. Purpose

This document provides members of projects using the Trustworthy Research Environment (TRE) with instructions on acceptable use of TRE equipment and assets, and procedural information for connecting to the TRE and accessing the data within it.

The TRE holds large amounts of confidential and sensitive information that must be treated with respect and integrity. It is the responsibility of all members of staff to protect information from inappropriate disclosure and access by adhering to this User Manual.

The TRE, and all systems contained within, is involved in handling information that must be managed in a way that ensures its confidentiality, availability and integrity. Implementing security controls throughout the lifecycle of a system can help the TRE achieve its ISMS objectives, regulatory requirements and the needs of its users.

2. Scope

This procedure applies to anyone who works on a TRE project or who is going to be provided with a TRE user account. It also applies to anyone who has access to the TRE computing resources, data or and related information assets, for example TRE Operations staff or contractors.

3. Responsibilities

The Information Security Manager (ISM) is responsible for:

- Investigating any usage not conforming to this policy
- Assisting the TRE Operations Manager in managing audit logs that may be needed to investigate non-conformances

The TRE Operations Manager is responsible for:

- Supporting the ISM with any actions and non-compliances arising from this policy
- Ensuring the appropriate legal and ISMS processes have been followed by TRE Operations staff, users, contractors, etc.

The TRE project members are responsible for:

- Providing evidence to support induction of the project's TRE users
- Reporting any concerns about data security
- Ensuring appropriate procedures are followed at all times

4. Procedure

The TRE comprises a highly scalable virtual machine environment, which includes dedicated network security and storage infrastructure. The primary role of the TRE is to provide data processing workstations to end-users, and for those workstations to have access to data that is stored securely within the TRE, and only made available to members of a project that the data belongs to.

These data processing workstations are provided as virtual machines. This means the researcher will use their own physical computer or laptop to connect across the network to their allocated virtual

data processing workstation within the TRE. They will have full control of the data processing workstation via a remote desktop interface. It will appear as if this data processing workstation is local to the user, but in fact there is a distinct 'air-gap' separating it from the local computer/laptop to limit data transfers in or out.

The virtual workstation (VM) is configured to meet the project requirements and user preferences. This is done as part of their initial account and project setup, and the user's local network and PC/laptop will have been added to the TRE's firewall whitelist.

4.1. TRE User Induction

A TRE User Induction must be completed before an individual receives TRE account details. Induction comprises document reading (see 4.1.1) and completion of a training course related to safe data handling (see 4.1.2).

The TRE user is responsible for providing evidence to tre-support@manchester.ac.uk that they have done this in the form of:

- A signed copy of the user agreement (see Appendix)
- Confirmation that that the documents have been read and understood*
- Confirmation of completion of the required training course, e.g. a certificate

* For those who have Q-Pulse access, a Q-Pulse document acknowledgement is accepted in place of this email.

4.1.1. TRE Documents

The Table 1 summarises which ISMS/TRE documents the TRE user must read and understand:

Document Name	Acknowledgement required declaring document has been read?	Signed/Completed document to be returned?
SOP-03-23 Using the TRE Secure Data Access Room	Yes	No
ISMS-03-02 TRE User Clear Screen and Desk Policy	Yes	No
ISMS-03-05 TRE Bring Your Own Technology Policy	Yes	No
ISMS-03-07 TRE Password Policy	Yes	No
ISMS-03-09 TRE Acceptable Use Policy	Yes	No
ISMS-07-04 Information Security Classification	Yes	No
SOP-02-02 Reporting Incidents	Yes	No
SOP-03-02 TRE User Manual and Agreement	Yes	No
SOP-03-11 Protecting the TRE from Malware	Yes	No

Table 1

There are also documents that may be needed at certain times of the project's lifecycle. It is not necessary to provide acknowledgement of having read them.

Document Name	Purpose
FORM-007 TRE Project Service Request Form	To be filled in and sent to the TRE Operations team if a change to the project is required, e.g. to add a new user
SOP-03-16 Connecting to TRE Linux machines with X2Go	How to install and setup X2Go on a Windows PC to enable remote connections to the TRE
SOP-05-03 Importing Datasets into the TRE	The procedure that must be followed by the Data Provider/Controller
SOP-07-02 TRE Data Export and Output Checking	Procedure for getting data out of the TRE

Table 2

4.1.2. Training Courses/Qualifications

Access to the TRE requires successful completion of at least one of the following training courses:

- Safe Researcher Training. This can be run locally – contact tre-support@manchester.ac.uk for the next date.
    - Sessions are also held by the UK Data Service or Office for National Statistics.
    - For background information see: http://blog.ukdataservice.ac.uk/a-new-integrated-approach-training-researchers-to-use-sensitive-microdata/
- MRC's 'Research, GDPR and confidentiality – what you really need to know' course (or equivalent approved by TRE Management): https://byglearning.com/mrcrsc-lms/course/index.php?categoryid=1

The TRE Operations team maintain a training record for each TRE User (for details see SOP-01-06).

4.2. Accessing data in the TRE

4.2.1. Approved data handling

Anyone responsible for bringing data into the TRE for their project must ensure the appropriate legal processes have been followed. For example, if the data has been supplied by a 3rd party, it may be necessary to conduct a privacy impact assessment or data sharing agreement with the data controller.

The Data Sharing agreement or contract between the user/project team and the Data Controller should specify the permitted use of the data that has been shared. The Centre for Health Informatics additionally requires all TRE users to sign the TRE User Agreement (see Appendix).

4.2.2. User connections to the TRE

Access to TRE data is first determined by the approved TRE project request (using document FORM-002) which lists all people who require a TRE account within that project. SOP-09-13 describes the technical controls that govern which data is made accessible to a TRE user.

Access to a virtual workstation is dependent on the operating system of the virtual machine (VM). The following table lists the supported types of connection:

User's operating system	TRE Virtual Machine operating system	Connection type	UoM VPN required?
Microsoft Windows	Microsoft (Windows 10 professional)	Microsoft Remote Desktop Connection with 2FA key	Yes*
Mac	Microsoft (Windows 10 professional)	Microsoft Remote Desktop (available from iTunes**) with 2FA key	Yes*
Linux	Microsoft (Windows 10 professional)	RDP client, e.g. Remmina / FreeRDP with 2FA key	Yes*
Microsoft Windows	Linux (CentOS 7)	SSH (for command line only, use Putty. For a 'Windows' graphical user environment, us X2Go). SSH key-pair required, created with puttygen.	No
Mac	Linux (CentOS7)	SSH. For a 'Windows' graphical user environment, us X2Go). SSH key-pair required.	No
Linux	Linux (CentOS7)	SSH. For a 'Windows' graphical user environment, us X2Go). SSH key-pair required.	No

* Users of a PC or laptop connected via a network cable to the University campus network will not need to use the VPN

** All RDP clients must support Network Level Authentication (NLA).

Whichever connection method a user chooses, connection should only take place from an authorized computer, for example a user's standard desktop. Users must never set up additional remote desktop connections to an authorized computer in order to access the TRE.

4.2.2.1. Connecting to VMs running a Microsoft operating system

The only method of connecting to a Microsoft Windows machine is via the RDP protocol using an RDP client. An RDP connection will first launch a prompt requesting a username and password (which will have been provided during the account registration process). If the account credentials are valid, a second prompt will appear requesting the numerical key that is displayed on the key fob. If the correct key is provided, the established connection will launch the remote desktop connection, which will either fill up the local screen entirely or partially depending on the local resolution.

4.2.2.2. Connecting to VMs running a Linux (UNIX) operating system

A command line interface or a graphical 'Windows' environment can be provisioned. Users can choose between these depending on the task to be carried out. The only permitted method of

connecting to a TRE Linux machine is via the SSH protocol. To operate an SSH connection from a Microsoft Windows machine, software called 'Putty' must be used. In its default configuration, Putty will only allow a command line interface to be viewed. If a graphical environment is required, software called 'X2Go' should be installed (clients are available for Microsoft Windows, Mac and Linux computers). A successfully established connection will result in the remote (TRE Linux VM) desktop being displayed locally. The TRE's Linux virtual machines are configured to provide the XFCE version of X-Windows. See SOP-03-16 for full details.

4.3. SSH Key-Pairs

To achieve 2-Factor Authentication (something you know + something you have on your possession) when users connect to a Linux machine, we use SSH key-pair sharing. This is where you:

- Generate an SSH key-pair, preferably on the same computer you will use to connect to the TRE. The approved tool for generating ssh key-pairs via Microsoft Windows computer is 'puttygen.exe'. This is something bundled into the full Putty download.
- Make a note of where you store your key-pairs.
- Send your public key to the TRE team to install this public key onto the Linux virtual machine allocated to you
- Configure your local SSH client (Putty or X2Go) to use the SSH key-pairs
- Your computer will connect to the TRE virtual workstation via SSH and the public key exchange validates the overall connection

4.4. Data Storage

Depending on the functionality specified during the account request, the remote desktop environment will provide local and/or networked data storage. On a Microsoft Windows remote workstation, local storage will reside within the C: partition (e.g. My Documents) and a networked storage resource will be made available via another drive partition (and assigned a letter such as 'R:' as specified during the account request).

4.5. Software Applications

There will also be software applications and tools installed on the virtual machine allocated to the user, as specified during the account registration. These applications will be able to read (analyse), modify (process) and save any derived datasets onto the internal networked storage allocated to that project

4.6. Restricted Usage

The following operations are disabled by default within the virtual machine desktop environment:

- Connecting to the internet (via any tool/protocol, e.g. web browser, email, ssh, ftp, remote desktop, database connection)
- Connecting to another virtual machine within the TRE
- Transferring data to an external repository or file sharing service such as DropBox (see ISMS-03-05 TRE BYOT Policy)

The following operations are disabled between your computer and the remote virtual machine desktop environment:

- Copying a local file or text from within a local file and pasting it into the remote desktop environment
- Copying a remote file or text from within a remote file and pasting it into the local desktop environment

The following additional functionality is also disabled:

- Printing
- Changing the username and/or password
- Modifying mount points to networked storage
- Depending on permissions assigned to a user, it may not be possible to create or modify files and directories within a network storage area

4.7. Using the Secure Data Access Room

Projects that require access to highly sensitive data, for example healthcare records containing personal identifiable information may need to connect to the TRE from the Secure Data Access Room. Document SOP-03-23 explains this resource in more detail.

4.8. Maintaining the Virtual Machine Status

The virtual workstations provided within the TRE will not:

- Automatically reboot due to software updates
- Automatically turn the screen off to save energy
- Automatically lock the screen and require a password to unlock
- Automatically set the virtual machine to 'sleep' mode or 'hibernate' mode

The user is permitted to reboot or shut down their virtual machine. If the virtual machine is shut down, it will be necessary to contact the TRE Operations Team to request that the virtual machine is booted back up.

4.9. Monitoring

All activity on/in the TRE may be subject to routine monitoring and measurement (SOP-04-04) in order to support the continual improvement of the TRE management system, and to monitor security breaches. Security breaches will be reported to the information security manager, and may get escalated to the University of Manchester Data Protection Officer, the Department of Health (DH), NHS England and the Information Commissioner's Office (ICO). See SOP-07-05: Escalation to IG SIRI.

4.10. Breaches of this policy

Breaches deemed to contravene acceptable use may result in one or more of the following:

- Re-training;
- Suspension of your TRE account;
- Permanent exclusion from the TRE;
- Possible prosecution (Taking action - data protection)

4.11. Collaborative Projects

In some cases, a number of virtual machines will be setup for a group of users, all belonging to the same project. In these cases, it will be possible to share a networked storage area between each of the virtual workstations allocated to the users (members) of that project. It might also be possible to host a database within the TRE that is only accessible to that group of users.

4.12. Getting Data into the TRE

The TRE operates strict rules governing the transfer of data in and out of the TRE (see SOP-05-03). Details of how data is brought into the TRE are discussed during the initial project application, and also during the setup of the overall project's working environment.

4.13. Getting Data out of the TRE

Raw data in the TRE will be destroyed when the corresponding user account and/or parent project expires. This raw data will not be transferred elsewhere, unless agreed during the project's application or subsequent approved requests (see ISMS-07-01).

Users can transfer processed or derived data out of the TRE, for example, onto a public data repository. This will involve review by the TRE Operations team to ensure that:

I. the data leaving the TRE is of an appropriate quality and level of identifiability
II. all necessary information governance procedures have been followed

When derived data or code needs to be exported from the TRE, for example for publication, output checks need to be done. This procedure and timescales are described in SOP-07-02.

4.14. Providing feedback to the TRE support team

Any user can contact the TRE support team by email: tre-support@manchester.ac.uk

5. Cross-referenced ISMS Documents

Number	Type	Title
SOP-05-03	ISMS\SOP\Asset and Supplier Management - SOP	Importing Content into the TRE
SOP-03-23	ISMS\SOP\TRE Operations - SOP	Using the TRE Secure Data Access Room
ISMS-03-05	ISMS\Policy & Guidance\TRE Operations - policy & guidance	TRE Bring Your Own Technology Policy
FORM-002	ISMS\Forms	TRE Project Application Form
SOP-04-04	ISMS\SOP\ISMS Improvement - SOP	ISMS Measurement and Monitoring
SOP-09-13	ISMS\SOP\TRE System Administration - SOP	TRE Access Control

SOP-03-16	ISMS\SOP\TRE Operations - SOP	Connecting to the TRE with X2Go
SOP-07-02	ISMS\SOP\Information Governance - SOP	TRE Data Export and Output Checking
ISMS-03-05	ISMS\Policy & Guidance\TRE Operations - policy & guidance	TRE Bring Your Own Technology Policy

6. Appendices

TRE User Agreement

Scope:
Trustworthy Research Environment ("TRE") Users must agree to this Service Agreement ("Agreement") and any other documents referred to herein before being granted access to TRE services and datasets.

1. Introduction

This document represents the final administrative step that prospective users of the TRE must fulfil before being granted access credentials to access data in the TRE. The Agreement is signed by the user and returned to TRE administrative staff prior to being given a username and password. The Agreement demonstrates that the user understands the seriousness of the undertaking, and that they and their institution understand the penalties that may be imposed for breaches of security or confidentiality.

2. The Parties

This Agreement is agreed between:

a. Individual user of the TRE
b. The University of Manchester ("University") Centre for Health Informatics

3. Definitions

"Approved Researcher" A researcher based at, or sponsored by, a higher education organisation based within the EU, who holds a current approved researcher qualification.

"TRE User" An Approved Researcher to whom the University and data owner has granted access to one or more datasets and/or services within in the TRE.

"Personal Information" Information that relates to any living individual (including corporate body) who can be identified from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

"Purpose" The particular research proposal approved by the data owners or their designated decision making body in the Approved Researcher application process.

"TRE" A service operated by the Centre for Health Informatics from Vaughan House, The University of Manchester. This service is intended to promote collaboration and excellence in health research by enabling a safe and secure remote access to data that may be deemed too sensitive, confidential or potentially disclosive to be made available under standard dissemination agreements.

4. Agreement

4.1 All TRE Users must satisfactorily complete mandatory training which allows the University to ensure that they are fully aware of their responsibility to data protection and the potential penalties for breaches of security, confidentiality or this Agreement. TRE Users will be required to re-attend training according the TRE requirements.

4.2 Access to Personal Information is being provided for health research Purpose outlined in the TRE Project Proposal form. Personal information shall not be used for any other purposes without prior written consent of University and data owner(s).

4.3 The TRE User shall not disclose nor compromise any of the Personal Information from access to individual records or datasets obtained or produced from the Personal Information pursuant to this Agreement to anyone other than those approved for the same research Purpose and TRE staff involved in the review of research outputs for statistical data control.

4.4 The User shall ensure that there are no attempts to link Personal Information to any other files in order to re-identify individuals, organisations or business unless such data linkage has been explicitly approved at the time of the TRE project application, or approved subsequently as part of a special request to the data owners or their decision making body.

4.5 On termination of this Agreement for whatever reason, all access to the Personal Information related to the Purpose shall cease forthwith, and electronic access be denied.

4.6 The university reserves the right to monitor, record, and audit, or request written report from the User regarding the use, and activities relating to the use, of the Personal Information by the User during the lifetime of this Agreement. This includes the right to access the site from where the data is accessed and the right to audit such premises.

4.7 It is the User's responsibility to ensure that any computer the use to access TRE services has anti-virus software installed which automatically updates on a daily basis. Before access is granted to TRE the User will be asked to provide information relating to their operating environment.

4.8 Any confirmed or suspected incidents of unauthorised access, use, disclosure or processing of Personal Information must be immediately reported to the University.

4.9 The Agreement is subject to review and without limitation whenever a change in the law, contracts for services with third parties, other procedures or other relevant circumstances takes place.

Output release

4.10 The user shall not reproduce to any extent from the TRE any original dataset, copy or subset of Personal Information.

4.11 Any outputs to be removed from the TRE must first be screened by TRE staff to ensure that the output is not disclosive of an individual, business or organisation. Outputs may be screened by other services, such as data providers or external auditors. Only screened outputs that are approved as being nondisclosive will be distributed to the User from the TRE.

4.12 Users are responsible for applying the rules and regulations for handling and processing Personal Information prior to submitting outputs for screening.

4.13 The User agrees to work with the University to produce safe outputs. In the event that the University decides to not release the proposed output, the user will be given opportunity to demonstrate that the output is safe. However, the final decision to release the output rests with the University.

4.14 The University reserves the right to release in whole or in part, an amended version or not to release at all, as the university deems appropriate, the proposed output produced by the principal investigator and their team pursuant to this agreement.

4.15 Users shall provide sufficient information about the variables used, new variables/measures/indices created, documentation of datasets and programs used in production of outputs(s) to ensure that the University has enough detail and sufficient time (at least 7 days) in order to make a judgement on output(s) put forward for release.

4.16 The User shall conduct secondary disclosure checks of outputs that are published together and inform the University of any publications that contain output(s) release by the TRE.

Acknowledgements and copyright

4.17 The Personal Information, datasets and related information shall at all times remain the sole and exclusive property of the data owner. This Agreement pertains to the production of health research outputs and that nothing herein shall be deemed to convey any title or ownership interest to the user.

4.18 Copyright of outputs may be held jointly or singly by the User(s) that created them, their institution(s) or their funder(s) according to the User's funding and institutional agreements.

4.19 The User must refer to the TRE in any publication as appropriate, for example referencing www.herc.ac.uk/tre in the Methods section or an endnote.

4.20 The User must acknowledge, in any publication that contains outputs released by TRE, whether printed, electronic or broadcast, the original data creators, depositors or copyright holders and funders.

4.21 The User must cite, in any publication that contains outputs released by TRE, whether printed, electronic or broadcast, the datasets used. The University can provide guidance on appropriate citation.

5. Declaration

By signing this Declaration you are confirming:

- You have read, understood, agreed and provided digital signing/acknowledgement to the following TRE documentation listed in Table 1 of the TRE User Manual
- The accuracy of the information in this Agreement
- You have read and understood the conditions in this Agreement
- You will comply with all of the policies and TRE operating procedures presented to you, including requirements relating to the use of potentially disclosive or Personal Information

I declare that the information provided to me shall be kept secure and confidential according to the terms of this agreement.
The University may hold and process information submitted by me in the TRE Project Proposal form for validation and for the purpose of the management of services and may also pass such information on to other parties such as data provider or auditors.
The University receive the right to review outputs for disclosure control purposes before publication.
I and my organisation may be liable for penalties as outlined in the Breaches Penalties Procedure if I disclose information without written authorisation from the University.
My lawful use of information is only for the research purposes as outlined in the study protocol and will serve the public good.
I am required to bring to the attention of the University any matters or events that may affect obligations under this declaration.

User's full name and title	
Institution	
Date form completed	
For non-University of Manchester applicants only:	
Institutional address	
Institutional authority signature	
Date of signature	
Name of institutional signatory	
Position of Institutional Signatory (must be a member or the research and contracts office, or equivalent and must have legal authority on behalf of the institution)	

By emailing this form to tre-support@manchester.ac.uk, the User is declaring their agreement with the terms of usage defined within this document.