STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Restricted

Title:	**Using the TRE Secure Data Access Room**
Effective Date:	**29 Aug 2019**
Reference Number:	**SOP-03-23**
Version Number:	**1.0**
Owner:	**Information Security Manager,**
Review Date:	**29 Aug 2021**

Table of Contents

1. Purpose

Physical security for offices, rooms and facilities should be designed and applied.

This document describes the Trustworthy Research Environment Secure Data Access Room (SDAR), the protocol for requesting access, and the terms and conditions for its use.

2. Scope

The Secure Data Access Room (SDAR) accessed from within room 2.007 at Vaughan House.

The key-safe located inside room 2.007 at Vaughan House.

3. Responsibilities

TRE User are responsible for:
- Signing in and out of the applicable log sheets when obtaining the door key from the key-safe, and also when entering/leaving the room
- Not using mobile devices in the room or taking notes without prior approval from a member of TRE staff
- Respecting the privacy of other users
- Remembering to ensure windows/doors are left locked when the room is empty

The TRE Operation Manager is responsible for:
- Ensuring the equipment provided within the SDAR, and all physical security controls are working correctly
- Managing room access requests and granting/removing access to TRE users
- Monitoring signing-in books for the room and door key to ensure compliance with this procedure (as part of Routine Measurement and Monitor for the TRE Physical Security process)

TRE Staff are responsible for:
- Assisting TRE users when accessing the room and using the physical workstations (when support is requested)

4. Procedure

4.1. Introduction

The SDAR is a highly secure research data analysis room that provides TRE users with a suite of physical workstations directly wired into the TRE and isolated from the University network. Each physical workstation can only be used to make a remote connection to virtual machines hosted on the TRE network. The purpose of the SDAR is to provide the optimum level of control to prevent any compromise to the confidentiality of personal identifiable information derived from TRE data, while at the same time providing TRE users with a familiar and practical working environment.

4.2. Access to the Secure Data Access Room

The SDAR door has 2 locks:

1) Standard ‘mechanical’ door key - The door keys are stored in key-safe ID ‘TRE-SAFE-02’. A 4-digit number is needed to open the key-safe.

2) ID card activated ‘maglock’ - Access rights have to be granted to an ID card before it can be used to activate the door’s maglock.

FORM-005 must be completed to request the digital code for the key-safe and also to request that access is granted to an ID card.

On certain occasions, unauthorised individuals such as University IT Services staff or contracted fire alarm testers will need to access the room. These individuals must be accompanied by a member of TRE staff at all times, and any TRE users present in the room must be provided with 1 hours’ notice that someone unauthorised will be entering. It therefore follows that TRE staff must ensure their visitors provide them with adequate notice of their arrival.

After the SDAR entrance door has been unlocked at the beginning of each day, it is not necessary for TRE users to continually lock and unlock the door each time they temporarily leave the room, as the card activated maglock provides adequate security on a temporary basis. It is only necessary to lock the door if a user has finished their work and is leaving and not returning, and there is no-one else in the room at the time they leave (the key must be returned to the key-safe and the relevant signing-out sheets completed).

When the person who first unlocked the door finishes their work and is leaving and not returning, they can pass the key onto another user, but both people must fill in and sign the corresponding log sheets.

In the event of maglock failure, the SDAR door must be locked by key whenever the room is left unoccupied.

4.3. Signing-in book/sheet

There is a signing in book that must be filled in by each person when they enter the SDAR. They must also sign out when they have finished for the day. It is not necessary to sign out if leaving the room for a short period of time, e.g. toilet break. If someone is going to be absent from the room for more than 1 hour, it is necessary to sign-out, and then sign-in again on return.

There is also a signing-in sheet for the key-safe containing the door keys. The first person of the day who gets the key to enter the SDAR will have to sign the sheet to state they’ve taken the key. If there is no-one else in the SDAR when they have finished for the day, the key must be returned to the key-safe and signed-out on the sheet. If there is someone else in the SDAR when the key-holder is finished for the day, they can pass the key onto this other person who must then sign the sheet to say they have the key, and the first occupant must sign-out to indicate they no longer have the key.

4.4. Windows and Blinds

If the room gets too hot, occupants are permitted to open the windows, but they must never be left open if the room is unoccupied. This means if anyone is in the room on their own, and they leave, they must first close any open windows, even if they intend to return within a few minutes.

The windows are to be left unlocked.

The blinds can be opened partially to let sunlight and air into the room, but must be left closed at the end of the day. This means the last person to leave must close them.

4.5. Physical Workstations

The SDAR provides physical workstations that are used to connect to remote systems within the TRE. All physical workstations run on a Linux operating system, and each user of the SDAR is provided with their own user account to log onto the workstation that has been allocated them by the TRE Operations Manager. These Linux workstations have no software installed or any internet access. The only functionality they provide is a Linux command line (Bash shell) that is able to connect to remote machines via SSH or RDP, or the X2Go software application that ports a remote graphical desktop via SSH. If authentication to remote TRE machines requires SSH key-pairs, these will be created in advance for users and the passphrase provided to them. Therefore users of the SDAR require some basic knowledge of operating a Linux PC and authenticating with remote machines.

It is strictly forbidden to download any data onto the physical workstations from the TRE. Furthermore, TRE users should not create and store files on the physical workstations as the operating system may get reinstalled at any time without notice being provided. It is also forbidden to plug any devices into the USB sockets, unless it is a device required for authentication to a remote server, and the use of this device has been approved with the TRE Service team.

4.6. Zones

The desk spaces are split into 4 ‘zones’, each of which contains one or more physical workstation that connects to a network location determined by the purpose of that zone. Access to, and use of the TRE from within each zone must abide by terms and conditions specific to that zone.

1. TRE Unmanaged Project Technical Administration (by special arrangement only) – University Network
2. TRE Unmanaged Project Technical Administration – HSCN (NHS) Network
3. TRE Managed Project Data Analysis – University Network
4. TRE System Administration – University Network

Description of each SDAR Zone:

Zone 1: There is one physical workstation which connected to the main TRE network. This workstation will be allocated a persistent IP address that can be used to create a 1:to:1 firewall rule on remote TRE machines belonging to the TRE Unmanaged Project.

Zone 2: There are three physical workstations, each of which is directly connected to an internal private network that only has access to the HSCN gateway.

Zone 3: There is a single workstation which is directly connected to the main TRE network but a 1:to:1 IP address rule restricts connections from this workstation to the managed project VM belonging to the user. Users of this workstation will use their own local Linux account to log onto the workstation, and this account will use its own SSH key-pairs to authenticate connections to the respective project VM.

Zone 4: There is a single workstation that can connect to any networked device on the main TRE network. Its IP address is used for 1:to:1 firewall rules throughout the TRE and where possible, connections are further authenticated by SSH key-pairs belonging to the System Administrator's account on that workstation.

Figure 1 depicts how the TRE is split into 2 separate network areas, and how the SDAR physical workstations are directly connected to these networks via internal cabling within the Vaughan House building.

The Secure Data Access Room at Vaughan House

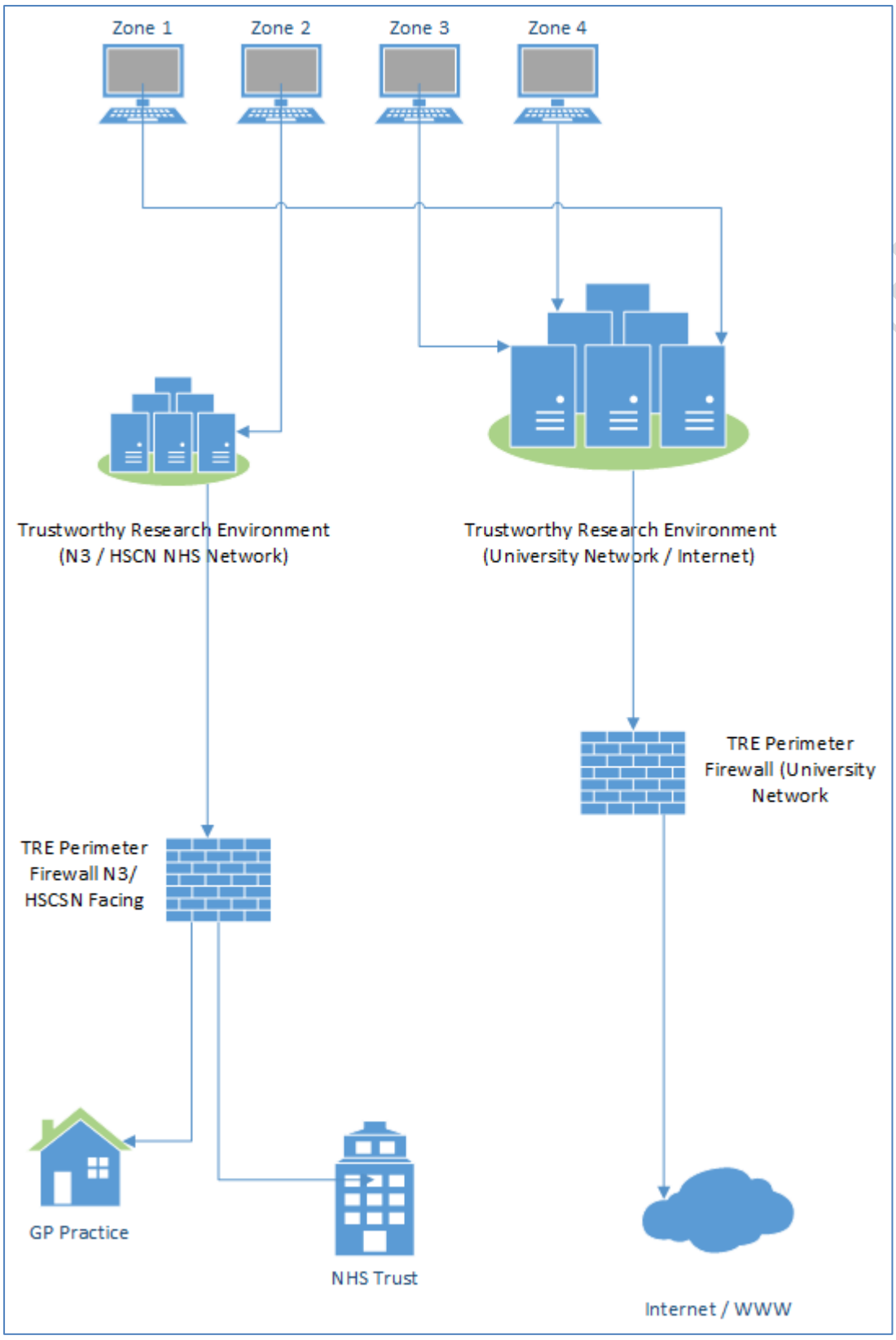

Figure 1

4.7. Agreed Usage of SDAR Zones

The following statements apply to TRE users and any other personnel entering the SDAR:

- The use of laptops, tablets, mobile phones or any electronic device that can store information or digital images is strictly forbidden within the SDAR. All such devices must remain in their owner's bag and not placed on the desks.

- Users needing to make a phone call or use their laptop must leave the SDAR and find a space within the building that will not disturb others, e.g. a corridor or the communal kitchen areas. The SDAR exits into an office so please try to remain silent so that no one is disturbed.

- If a user needs to make paper-based notes while working in the SDAR, this must be agreed in advance with a member of TRE staff so that the content can be checked before it is taken out the room (following the TRE Output Checking procedure). but these should not be taken out of the room without inspection by a member of TRE Staff.

The TRE System Administrator is exempt from the above rules if it is essential for TRE maintenance or user support.

4.8. Enforcement of Room Usage

TRE Staff reserve the right to check that users of the SDAR are complying with this procedure, which may include checking that mobile devices are not being taken out of bags and inspection of any paper-based notes.

4.9. Monitoring of Room Usage

The TRE Service team reserves the right to monitor all network traffic between the physical workstations and the TRE, and to retain event logs pertaining to this traffic. The event logs of each physical workstation will also be retained. Event log data will be retained for a period of time as specified in the TRE Log Management policy.

The SDAR features a CCTV system. The video cameras cannot view the workstation display monitors. Footage captured by this system will only be viewed following a suspected security incident. CCTV footage will be retained for a period of 12 months and stored securely within a TRE safe.

5. Cross-referenced ISMS Documents

Number	Type	Title
SOP-07-02	ISMS\SOP\Information Governance - SOP	TRE Data Export and Output Checking
SOP-03-02	ISMS\SOP\TRE Operations - SOP	TRE User Manual and Agreement

6. Appendices

None.