STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Restricted

Title:	**TRE Access Control**
Effective Date:	**07 Jun 2019**
Reference Number:	**SOP-09-13**
Version Number:	**1.4**
Owner:	**TRE Infrastructure and Security Management Process Owner,**
Review Date:	**09 Nov 2019**

Table of Contents

1. Purpose

This document describes the procedure for controlling remote access to digital content within the TRE. This includes placing restrictions on the source of remote connections and ensuring that users are only given permission to access content that they are authorized to access.

The Trustworthy Research Environment (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

All TRE infrastructure including servers, virtual workstations, network devices and user end-points

3. Responsibilities

TRE Operations are responsible for:

- Receiving requests and sending notifications related to access control to TRE Project Users and TRE Staff.
- Recording and checking information necessary for Information Security Manager (ISM) approval.

The Information Security Manager (ISM) is responsible for:

- Approving changes to access control.

System Administrators are responsible for:

- Implementing changes to access control.

Project Principal Investigators are responsible for:

- Informing TRE Operations of any changes to project users roles (for example, contract termination), such that access control should be changed.

Line Managers of TRE Staff are responsible for:

- Informing TRE Operations of any changes to staff roles (for example, contract termination), such that access control should be changed.

4. Procedure

TRE Project Users can access virtual machines and the services that they host, and TRE Staff can access virtual machines and core infrastructure. This procedure is for controlling this access by managing four key areas: end-points, protocols, user accounts and security groups; each are described in the following sections.

4.1. End-point control

Any remote connections into the TRE must be restricted to be from a specific source. This significantly reduces the likelihood of a successful intrusion. There are three firewalls that block connections by

default: the border firewall that is used to manage connections to the entire TRE infrastructure; the OpenStack firewall that is used to manage access to the OpenStack infrastructure; and guest firewalls that are used to manage access to single machines. This tiered structure provides a maximum level of security with the flexibility to secure different parts of the TRE according to policy. Users are only able to connect from machines with IP addresses added to a white list by System Administrators.

4.1.1. Project users

Before a virtual machine or any project managed services can be remotely accessed by a project user, the following steps must be taken:

1. Information about the remote client machine and the TRE virtual machine must be provided by the project Principal Investigator (PI). This information must include:
    a. The TRE Project ID
    b. The name of the virtual machine that the user will connect to
    c. The port range that the user will connect to
    d. The IP addresses of the remote machines that the user will connect from
    e. The date after which the IP addresses should be allowed
    f. The date after which the IP addresses should be blocked
    g. For access to resources managed by the TRE, the full name and email address of the person that will connect
2. TRE Operations will record connection details;
3. The ISM will approve connection from the remote machine;
4. At the start date, a System Administrator will update the firewall rulesets to allow connections from the remote machine.

System Administrators review the status of firewall rules and update the firewalls to block new connections from remote machines after their expiry date. Person details are only required for access to resources managed by the TRE, including SSH access to virtual machines. Person details are not required to provide access to services that are the responsibility of project staff, including web applications that are hosted on TRE virtual machines.

4.1.2. TRE Staff

Before any virtual machines can be remotely accessed by a member of TRE Staff (System Administrators or Content Checkers), the following steps must be taken:

1. The staff member must send the IP address of the remote client machine to TRE Operations;
2. TRE Operations will record the IP address;
3. The ISM will approve connection from the remote machine;
4. At the start date, a system administrator will update the firewall rulesets to allow connections from the remote machine.

The core infrastructure can only be accessed by TRE Staff from the Secure Data Room, and for this type of access, no client IP addresses need to be provided.

System Administrators review the status of firewall rules and update the firewalls to block new connections from remote machines after their expiry date.

When a staff member has an unexpected change of circumstance such that their job role changes, it is the responsibility their Line Manager to inform TRE Operations. TRE Operations will then record a change to the expiry date of the connection rule, approval will be sought from the ISM and, when approval has been given, a System Administrator will update the firewalls to block new connections after the expiry date.

4.1.3 Isolation

The TRE virtual machines are isolated from each other on the TRE internal network. It is not possible for project users to connect from one virtual machine to another using internal IP addresses. Connections can only be established from requested and approved IP addresses and ports. Isolation is tested after the initial setup of project virtual machines.

4.2. Protocol

The TRE managed virtual machines and core infrastructure can only be accessed using Secure Shell. This is a widely accepted secure network protocol for accessing remote machines. Before a user can access the machines using SSH, they must send the public key of an RSA 2048 bit key pair in OpenSSH format to TRE Operations. This key will be recorded, and the user will only be able to remotely connect to virtual machines using the corresponding private key. The user must notify TRE Operations of any key changes, sending the corresponding public key. User can connect to the TRE using SSH with a desktop environment using the X2Go tool (Connecting to Linux machines with X2Go SOP).

The default method of accessing TRE unmanaged virtual machines is using Secure Shell. Additional methods may be established by project users.

4.3. User Accounts

4.3.1. Linux Virtual Machines

4.3.1.1. Project Users

Before a project user can connect to a Linux virtual machine, an account must be created using the following steps:

1. The PI must provide the following information to TRE Operations for each account:
    a. The TRE Project ID;
    b. The name of the virtual machine on which the account should be created;
    c. The date the account should be activated;
    d. The date the account should be expired;
    e. The full name of the person that will use the account;
    f. The email address of the person that will use the account;
    g. Whether the user requires elevated permissions.
2. TRE Operations will record the information provided by the PI;
3. The ISM will approve the creation of the account;
4. A System Administrator will create the Linux account on the virtual machine, set the expiry date and activate the account at the start date.

Before each account is created, TRE Operations will ensure that there is a record for the account user in Q-Pulse, the user's training meets requirements and all necessary agreements have been received.

The first time a Linux account is created for a user, a unique username, user ID (UID) and group ID (GID) are assigned to this user and recorded alongside the user's SSH public key (see section 4.2) in the Linux User Register. If accounts are required for the same user on different virtual machines, the same username, UID, GID and public key are used. Project user UIDs and GIDs start at 10000; IDs below this value are for TRE staff and system groups.

TRE Operations regularly review the status of the accounts and send expiry warnings to users of accounts that are due to expire.

4.3.1.2. Administrators and content checkers

User accounts must be created on each virtual machine for each member of TRE Staff that is a System Administrator or Content Checker at the VM start date. The list of staff with these roles can be found in the TRE Staff Roles Register. The ISM must approve the creation of these accounts. Each administrator is granted sudo privileges to enable full administration of the VM.

System administrators regularly review the accounts and deactivate accounts on the expiry date. Linux accounts are never deleted to ensure a full audit trail. TRE Operations send Principal Investigators and account users notification when accounts have expired.

4.4. Security Groups

4.4.1. Linux Virtual Machines

Each TRE user has exclusive access to a personal folder on each virtual machine. In addition, there are three security groups that determine the permissions of users for other folders:

project - TRE project users are a member of this group. This provides full permissions to a shared folder.

checker - TRE content checkers are members of this group. Each virtual machine has restricted folders for importing and exporting content. Members of this group have read only permissions for content in these folders.

wheel - TRE project users that require elevated permissions are added to this group.

4.5. Exceptions

When a TRE user has an unexpected change of circumstance, for example their job role changes, it is important that TRE Operations are informed as soon as possible so that changes can be made to access control. TRE Operations will then record a change to the expiry date of any approved connections and virtual machine accounts associated with the user. For TRE Staff, TRE Operations will update the TRE Staff Roles Register accordingly. When approval of the change has been given by the ISM, a system administrator will update the firewalls to block new connections after the expiry date and set new expiry dates for the virtual machine accounts.

For Project Users, it is the responsibility of the project PI to inform TRE Operations. It is the responsibility of Line Managers to send notification of changes for TRE staff.

5. Cross-referenced ISMS Documents

Number~~Number~~	Type~~Type~~	Title~~Title~~
SOP-03-24	ISMS\SOP\TRE Operations - SOP	Migrating Projects out of the TRE
SOP-03-02	ISMS\SOP\TRE Operations - SOP	TRE User Manual and Agreement

6. Appendices

None