**STANDARD OPERATING PROCEDURE**
**Do not Photocopy**

**Document Information Classification: Restricted**

| | |
|---|---|
| **Title:** | **Creating Linux User Accounts** |
| **Effective Date:** | **05 Jul 2019** |
| **Reference Number:** | **SOP-09-01** |
| **Version Number:** | **1.4** |
| **Owner:** | **TRE Infrastructure and Security Management Process Owner,** |
| **Review Date:** | **28 Apr 2020** |

**Table of Contents**

## 1. Purpose

A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.

This document provides guidance to TRE system administrators for the creation and configuration of user accounts on Linux machines.

## 2. Scope

All users accounts for people who need to log onto a Linux machine.

This document does not cover creation of accounts used between services, for example, database user accounts.

## 3. Responsibilities

TRE System Administrators (SA)

- Ensuring all Linux virtual machine images provide the tools and support the configurations described within this document
- Ensuring that each user account is assigned the correct permissions

## 4. Procedure

The overall procedure is performed by a member of the TRE Operations team, by logging in with their own user account, and elevating their privilege to root via 'sudo' where necessary.

The steps covered are: account creation, setup of user's home directory, importing the user's ssh public key and converting to correct format, and setting up permissions/ownership of the user's home directory.

For the purpose of this document, a TRE user account is being created for the fictitious user with username 'rt56jh33'

a. Refer to the TRE Infrastructure Record to obtain the user's 8 character UNIX username (in this example it is 'rt56jh33')

b. Type that username into the command line and hit 'enter' to ensure it isn't also a valid command to run a program, or start a service

c. Assuming the result of 'b' is 'Command Not Found', create the user account with:

```
[bg@tre-project-vm-001 ~]$ sudo useradd rt56jh33
```

d. Create a password for this user account by providing it when prompted:

```
[bg@tre-project-vm-001 ~]$ sudo passwd rt56jh33
```

Note: as the use of ssh key-pairs is mandatory, the user won't be asked for this Linux user account password, and only the passphrase associated with their ssh key-pair. However, the account password may be required for administrative purposes.

e. Create a folder to store the user's ssh public key with:

```
[bg@tre-project-vm-001 ~]$ touch /home/
rt56jh33/.ssh/authorized_keys
```

f. Using WinSCP, import the user's public ssh key onto the machine, and place this in /home/js/.ssh

g. If Putty Key Generator was used to create the key pair, and export the public key, it will need to be converted once on the Linux machine using:

```
[bg@tre-project-vm-001 ~]$ ssh-keygen -i -f .home/
rt56jh33/.ssh/public-key-file-old > ~/home/
rt56jh33/.ssh/public-key-file-new
```

h. Import this public key into the authorized_keys file with:

```
[bg@tre-project-vm-001 ~]$ cat /home/ rt56jh33/.ssh/public-
key-file-new >> /home/ rt56jh33/.ssh/authorized_keys
```

i. Assign the permissions and ownership for the user's home area:

```
[bg@tre-project-vm-001 ~]$ chmod 600 /home/
rt56jh33/.ssh/authorized_keys

[bg@tre-project-vm-001 ~]$ chown rt56jh33:rt56jh33
/home/rt56jh33/.ssh/authorized_keys
```

## 5. Cross-referenced ISMS Documents

| Number | Type | Title |
|---|---|---|
| SOP-09-14 | ISMS\SOP\TRE System Administration - SOP | Secure File Transfer client setup |

## 6. Appendices

None