POLICY AND GUIDANCE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**TRE Password Policy**
Effective Date:	**07 Jun 2019**
Reference Number:	**ISMS-03-07**
Version Number:	**1.12**
Owner:	**Information Security Manager,**
Review Date:	**09 Oct 2019**

Table of Contents

1. Purpose

Users should be required to follow the organization’s practices in the use of secret authentication information.

The purpose of this document is to provide a standard for the creation, protection and frequency of change for passwords used under the scope of the TRE.

2. Scope

All individual, group and administrative passwords used for account authentication within the TRE infrastructure (TRE user accounts and infrastructure administration).

All passwords used to protect encryption keys used in conjunction with TRE access (e.g. SSH key-pairs) or for the secure storage of data.

Passphrases used in conjunction with SecurID tokens are not within the scope of this policy.

3. Responsibilities

The TRE Operations Manager is responsible for:

- Ensuring the validity of administrator account passwords
- Ensuring the validity of administration encryption key passwords

TRE System Administrators are responsible for:

- Configuring account management systems within the TRE to reject the creation of new passwords that don’t comply with this policy
- Resetting passwords on systems that do not allow users to manage their own passwords
- Only providing passwords to users via approved secure routes
-

TRE users are responsible for:

- Protecting their passwords
- Reporting security breaches involving passwords

4. Procedure

4.1. Introduction

There are three types of password (or passphrase) used with connections to the TRE:

1) Windows or Linux user account password
2) SSH key decryption passphrase
3) Passphrase or PIN associated with 2-factor or VPN authentication.

All connections to TRE Linux machines require the use of SSH key-pairs. SSH private keys are stored encrypted with a passphrase, so it is necessary to decrypt the private key when it is used for authentication. Even though a Linux user account comprises a username and password, connections to TRE Linux machines only prompt the user for their SSH private key decryption passphrase.

4.2. Password Requirements

All account passwords used and created under the scope of the TRE shall be created using the strong password criteria outlined below:

- Minimum length of 10 characters. The use of longer passwords is encouraged (up to a max of 16 characters).
- Case sensitive.
- Format must include a mixture of alphabetic (A-Z, upper and lower case), numeric (0-9) and special characters from the range: ! @ # $ % ^ & + = / ? [ ] . , _ ~ - unless prohibited by the software.
- Password expiry is defined by relationship with the TRE: when all relevant relationships end, access is revoked.
- Change frequency is not enforced apart from specific sub groups.
- Changes will be required and enforced if deemed a necessary risk treatment action.
- Inclusion of personal information in passwords is discouraged and may be prevented by software.
- Use of passwords that are considered to be risky may be prevented by software (blacklisting).

Further guidance can be found in the appendix of this document.

4.3. Management and Protection of Passwords

All individual, group and administration passwords are regarded as "Highly Restricted", this is the highest information confidentiality classification (see ISMS-07-04 Information Security Classification). All TRE users are responsible for management of their own passwords. Replacement passwords may be requested directly from software that supports "Forgotten Password" features; when this feature is not available the user may request their password to be rest by the software/system administrator. The replacement password, or password link, will require the user to define their new password upon the next login.

Group passwords may be shared securely within the group to which they belong. Group passwords shall be changed if a group member leaves the group.

The following guidelines shall be applied to passwords used under the scope of the TRE:

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to your colleagues
- Don't reveal your password to IT staff
- Don't reveal your password in service or help desk queries
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members or friends
- Don't enter your password into web sites that lack encrypted connections (no 'https://' in their address)
- Don't use your password with websites that show certificate warnings.

- Passwords can be recorded in a secure password management software tool that is encrypted and must be protected by a strong password conforming to this Policy. The TRE Service team recommend KeePass: https://keepass.info/
- Passwords should only be written down if they are stored securely under lock and key, for example in a safe with restricted access.
- Do not store passwords on your desk, in your desk furniture or under/in office equipment.
- Do not store passwords in a file on ANY computer system (including phones and other mobile devices) without encryption.
- On ANY device, encrypted or not, do not store passwords in a plain text file within the same directory as a component used for authentication, for example, an SSH private key or a VPN certificate.
- Do not use autocomplete for usernames and passwords
- The use of "save my password" functions is not permitted.

4.4. Frequency of Password Changes

It is recommended that passwords are changed every 12 months; however, you will not be prompted to update your password unless required by incident management or risk treatment.
Requiring a strong password and not requiring it be changed is regarded as more secure than the risks associated with changing passwords, such as the adoption of weaker passwords and risks of writing them down insecurely.

4.5. Backup of Critical Passwords

Passwords deemed to be of high importance, such as system administration passwords, shall be recorded on paper and will be securely stored in the fireproof safe, asset ID TRE-SAFE-01. The safe will only be accessed by approved staff, such as the ISM, ISMS Manager and ISSG members.

Each time anyone accesses TRE-SAFE-01 this must be recorded in the logbook which sits adjacent to the safe.

Each critical username and associated password shall be stored in a sealed envelope with the date of sealing and the name of the responsible person written across the seal. A new envelope shall be created each time the password is changed. Routine checks shall ensure that these passwords are still correct. This system has been implemented to protect critical passwords from being forgotten or lost, whilst ensuring that they are only accessed by key personnel.

5. Cross-referenced ISMS Documents

Number	Type	Title
ISMS-07-04	ISMS\Policy & Guidance\Information Governance - policy & guidance	Information Security Classification
SOP-03-16	ISMS\SOP\TRE Operations - SOP	Connecting to the TRE with X2Go

SOP-09-14	ISMS\SOP\TRE System Administration - SOP	Secure File Transfer client setup

6. Appendices

6.1. Examples of weak and strong passwords

Weak example	Strong example*
<10 characters	10-16 characters
Any single word in the dictionary	Combinations of 2 or more words, or a word not found in any dictionary, jargon or slang
Contains personal or company information (e.g. dates of birth, company name)	Contain alphanumeric characters, symbols and punctuation
Commonly used words, characters, pet names, dates	A phrase or sentence represented by letters, numbers and punctuation
Commonly used sequences: 1234, 0987,qwerty, qazmlp etc…	A phrase that has meaning to the individual creating the password, represented by a combination of letters and symbols. E.g. 2_B/n2_B!!

*any passwords provided in this table are for example purposes only and should not be used by any TRE user.