STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Restricted

Title:	**Testing Continuity of TRE Security**
Effective Date:	**07 Jun 2019**
Reference Number:	**SOP-09-17**
Version Number:	**2.0**
Owner:	**Information Security Manager,**
Review Date:	**13 Jun 2020**

Table of Contents

1. Purpose

Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions. The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

This document provides guidance for the tests that must routinely conducted to ensure any changes or events have not compromised information security within the TRE and recovery mechanisms are effective for the highest risk information assets.

2. Scope

This procedure focuses on the TRE Data including system configuration, user data and encryption keys as this represents the areas of highest risk to information security

Restoring data from backups is the most likely scenario to be managed following an adverse situation so the scope of this procedure is restricted to testing TRE data restores.

3. Responsibilities

The TRE Operations Manager is responsible for:

- Ensuring the TRE infrastructure record contains details of all tests conducted.

4. Procedure

4.1. TRE Data Restore

There are three types of data object within the TRE that are currently backed up routinely: *Encryption Keys*, *Storage Volumes* (user data) and *System Configuration*.

The procedure to test that a backed up data object can be restored differs between each item:

- **Encryption Keys**
  - Restore encryption key-file into an existing VM instance. Check that the VM can decrypt/mount an existing volume.
- **Storage (User data)**
  - Restore data volume. Mount a virtual machine to this restored data volume and verify its integrity.
- **System Configuration**
  - Restore the configuration item and rebuild the dependant component and verify. *Currently in the absence of a test environment, it is too risky to conduct these tests.*

4.2. Restoring Data Backups

Data is backed up and restored in accordance with the TRE Data Backup Policy (ISMS-09-11)

4.3. Frequency of Testing

Testing will be conducted every 2 months, in accordance with Routine Measurement and Monitoring (SOP-04-04).

4.4. Maintaining Record of Testing Events

The TRE Infrastructure record contains 3 worksheets for the following data restores:

i) Encryption Key Restore
ii) Storage Restore
iii) Config Restore

Each time a test is conducted, an entry will be placed in the Infrastructure Record (REC-001).

5. Cross-referenced ISMS Documents

Number	Type	Title
REC-001	ISMS\Record	TRE Infrastructure Record
SOP-03-08	ISMS\SOP\TRE Operations - SOP	TRE Change Control
ISMS-03-03	ISMS\Policy & Guidance\TRE Operations - policy & guidance	TRE Disaster and Severe Incident Recovery Plan

6. Appendices

None