POLICY AND GUIDANCE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**TRE Data Backup Policy**
Effective Date:	**20 May 2019**
Reference Number:	**ISMS-09-11**
Version Number:	**1.5**
Owner:	**TRE Infrastructure and Security Management Process Owner,**
Review Date:	**18 May 2020**

Table of Contents

1. Purpose

Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.

This document provides guidance for the backup and recovery of digital data assets within the Trustworthy Research Environment (TRE).

2. Scope

This policy provides guidance for the backup and restoration of TRE digital content, covering content imported into the TRE and content related to the state and configuration of the TRE infrastructure.

3. Responsibilities

TRE Operations are responsible for:

- Receiving requests and sending notifications to TRE Staff and users.

The Information Security Manager (ISM) is responsible for:

- Approving backups and restorations.

TRE System Administrators are responsible for:

- Ensuring that digital content are backed up and can be restored in the event of accidental loss or system re-installation or configuration.

TRE Staff and TRE users are responsible for:

- Making requests using an established email address for the TRE Support Team.

4. Policy

All digital information systems are exposed to the risk of data loss from accidental deletion or corruption due to infrastructure errors. This guidance aims to establish best practice for ensuring TRE digital content are appropriately backed up a way that allows appropriate and effective restoration:

- All data and system configuration files required in the event of system re-installation and or configuration must be backed up.
- Full backups of all data and system configuration files are performed weekly. Incremental backups are performed daily. Backups are retained for 25 days before being overwritten.
- Backups are held on the storage controller in the TRE Server room. There is currently no offsite storage for backup.
- Records will be maintained that provide information about backup and restoration activities that provide a full audit trail.
- Backup restoration checks will be performed to ensure that data can be successfully recovered from backups. Records will be maintained to provide information about each check. The ISM must be notified immediately if there are problems restoring backups.
- Backups must be encrypted. Encryption keys must be kept in a secure location and be uniquely identifiable.
- Physical access to onsite backup systems must be restricted to authorized personnel only.

- All backups that require long term archival will be stored at secure remote locations with appropriate controls to ensure the integrity of backup media.
- Backup media that are no longer required must be clearly marked and disposed of according to SOP-05-02 Return, Re-Use and Disposal of TRE assets.
- When TRE Staff require data to be restored, they must contact TRE Operations by email using tre-operations@manchester.ac.uk. Requests will only be approved for individuals that are authorized to access these data.
- When TRE users require data to be restored, they must contact TRE Support by email using tre-support@manchester.ac.uk. Requests will only be approved for individuals that are authorized to access these data.
- TRE Operations will establish if a user requesting a restoration is authorized to access the relevant files.
- Users that require data to be restored must provide sufficient information to allow the data to be correctly identified. This information must include:
    - The reason for the restore
    - The name of the files and folders
    - The original location of the files and folders
    - The earliest date and time that the data were lost (for example, from deletion or corruption)
    - The most recent date and time that the data were last in the correct state

5. Cross-referenced ISMS Documents

Number	Type	Title
SOP-05-02	ISMS\SOP\Asset and Supplier Management - SOP	Return, Re-use and Disposal of TRE Assets

6. Appendices

None