POLICY AND GUIDANCE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**TRE Bring Your Own Technology Policy**
Effective Date:	**07 Jun 2019**
Reference Number:	**ISMS-03-05**
Version Number:	**1.11**
Owner:	**Information Security Manager,**
Review Date:	**10 Oct 2021**

Table of Contents

1. Purpose

A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.

CHI recognises that staff and TRE users will use their personal devices to carry out their work which can create information security issues.

This procedure describes the terms of usage for BYOT that is permitted to access the TRE and TRE assets.

The term BYOT has a similar meaning to BYOD (Bring Your Own Device) but additionally covers technologies such as cloud compute/storage services. BYOT refers to personally owned computing resources: *workstations, mobile phones, laptops, tablets, portable hard drives, USB memory sticks* and other devices/services used to *store* or *access* electronic data for example, cloud storage.

2. Scope

TRE user account owners, while connecting to a TRE virtual workstation, or any service hosted within the TRE core infrastructure.

Only BYOT workstations and laptops (Windows, Mac or Linux) used to connect to the TRE or to operate the Q-Pulse client are supported under this policy.

All other BYOT is considered out of scope of this policy.

3. Responsibilities

TRE Staff and TRE users are responsible for:

- Configuring their computing/mobile devices to meet the requirements described below under the heading 'Security Configuration'

4. Policy

4.1. Terms of TRE Access via BYOT devices

As specified in the TRE User Manual (SOP-03-02) it is not permitted to connect to the TRE with mobile phones and tablets, nor can portable storage devices be used (as TRE users cannot upload/download data themselves), and therefore the use of such devices is not supported by this policy.

Furthermore, within the context of a research project that has been allocated TRE access, and due to strict firewall rules within the TRE, it is not possible to supplement TRE resources by using 3rd party computation/storage services such as Amazon AWS or DropBox. The exception to this rule is for the management of derived datasets (validated and authorised for extraction from the TRE) that do not contain any identifiable or sensitive information, as determined by the Information Classification policy (ISMS-07-04) and where suitable permission for the extraction of that data has been obtained.

4.2. Implementation of Security Controls

Individuals who wish to make use of BYOT to connect to the TRE/TRE Assets must take responsibility for ensuring that their device has appropriate information security controls by:

- Familiarising themselves with their device and its security features so that they can ensure the safety of TRE information (as well as their own information)
- Invoke the relevant security features
- Maintain the device themselves ensuring it is regularly patched and upgraded
- Ensure that the device is not used for any purpose that would be at odds with the TRE information security polices and local organisational policies
- Ensure suitable anti-virus software is installed and operating, and frequently updated to obtain the latest virus definitions. If necessary, the University of Manchester offers its staff and students a licensed copy of Sophos Antivirus which can be installed on a BYOT workstation or laptop. Details of how to obtain Sophos are described in the UoM instruction Anti virus software.

4.3. Security configuration and device usage

All BYOT owners must:

- Lock the screen when their computing/mobile device is not in use, or when leaving the device unattended
- Configure the security settings of their computing/mobile devices such that it is always necessary to provide a password after the screen has been unlocked, the device brought out of 'sleep' or 'hibernation' mode, rebooted or booted up from shutdown
- Configure their devices to lock the screen automatically if left idle for 5 minutes or less

All BYOT owners must not:

- Store copies (e.g. screenshots, downloads, scanned images etc.) of personal identifiable information, or business critical information.
- Use an inbuilt camera to gather sensitive information either by photographing a computer screen or printed material.

4.4. Connecting BYOTs to TRE Assets

Connecting BYOTs directly to TRE assets, for example by USB port, is not permitted unless prior approval has been granted by the TRE operations team.

4.5. Use of BYOTs in the Secure Data Access Room

The use of BYOTs in the TRE Secure Data Access Room is strictly prohibited. No member of staff or TRE user is permitted to use BYOTs in this room.

4.6. Breaches of this policy

TRE data must be processed in accordance with the Data Protection Act 1998. A breach of the Data Protection Act can lead to the University being fined up to £500,000. Any member of staff found to have deliberately breached the Act may be subject to disciplinary measures, having access to the University's facilities being withdrawn, or even a criminal prosecution.

4.7. Additional guidance

CHI strongly advises against the use of Rooted (Android) or jailbroken (iOS) devices. Additionally, mobile software applications from sources other than Google Play (Android) and iTunes (iOS) should be avoided.

5. Cross-referenced ISMS Documents

Number	Type	Title
SOP-03-02	ISMS\SOP\TRE Operations - SOP	TRE User Manual and Agreement
ISMS-07-04	ISMS\Policy & Guidance\Information Governance - policy & guidance	Information Security Classification
SOP-03-02	ISMS\SOP\TRE Operations - SOP	TRE User Manual and Agreement

6. Appendices

None