MANCHESTER 1824
The University of Manchester

Technical Security Standard

Title:	**Minimum Controls TSS**		
Version:	**1.1**	**Effective Date**	**July 2018**
Summary:	**This Standard defines the minimum baseline security controls and processes required for a given Information Security Classification.**		

When using this document please ensure that the version you are using is the most up to date by checking on the University's online document system http://documents.manchester.ac.uk/list.aspx for any new versions.

1 Introduction

This document is a Technical Security Standard and as such describes security control requirements. Detailed configuration and implementation requirements should be contained within operational procedure and guidelines documentation. The controls in this Standard MUST be implemented in accordance with local legislation; legislative, regulatory or 3rd party agreements may impose additional controls, which take precedence over this standard.

2 Purpose

The University handles a wide variety of information which is often shared internally and with outside organisations and individuals. Appropriate baseline controls are required which are commensurate with the selected Information Security Classification for an asset. This document provides the technical definition of those minimum controls.

3 Audience

This document is intended to be read primarily by Solution Architects, members of the Security Operations Centre, system administrators responsible for IT services infrastructure and applications and Risk and Compliance staff.

The standards contained in this document will apply to all University systems whether directly managed by University staff or the responsibility of an outsourced supplier. The principles described in this document provide minimum baseline protection for the University environment against potential unauthorised data modification and/or access. Any exceptions to these standards MUST follow a formal exception processes with appropriate risk acceptance and approval.

4 Definitions and scope

In this document the terms **MUST** and **SHOULD** are used and when in upper case have the following meaning (as detailed in RFC2119): -

- **MUST** means mandatory, is an absolute requirement.
- **MUST NOT** means forbidden – is an absolute prohibition.
- **SHOULD** and **SHOULD NOT** means an exception should be raised by management and approved by the Head of Information Governance (HOIG) if the requirement or prohibition is not met.
- **MAY** or the adjective "OPTIONAL", mean that an item is truly optional.

Information - For the purposes of this Procedure, information includes the raw data from which information is derived.
Information Asset - An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.
Information Asset Owners ("IAO") - IAOs are accountable for the information being processed. Where information is created and accessed by many users (such as the University's administrative applications) the Information Asset Owner is the business owner for the service. Information Asset Owners also include, for example, the authors of research papers, dissertations, databases or spreadsheets (this list is not intended to be exhaustive).
Information lifecycle – the information lifecycle describes the stages a record or piece of information goes through, from creation through being an active record (i.e. one which is used on a regular basis) to a semi-active record (one which needs to be kept but which is less frequently used) to disposition (archiving, destruction).

Scope: All information created or received in the course of University business which must be protected according to its sensitivity, criticality, and value, regardless of the media on which it is stored, the location of the information, the manual or automated systems that process it, the methods by which it is distributed or the locations from which it is accessed.

5.1 Information Security Classification

Information Security Classification is carried out according to Information security classification, ownership and secure information handling SOP

5.1.1 Unrestricted

- No technical security controls are defined for Information that is Classified as Unrestricted. Additional controls MAY be implemented as desired by the IAO.

5.1.2 Restricted

- Authentication SHOULD be carried out against a University IT Services operated Identity Provider, in compliance with the Authentication TSS.
- Information not protected by non-replayable authentication SHOULD NOT be directly accessible from the public Internet.
- Encryption SHOULD be applied in compliance with the Encryption TSS.
- Logging and audit controls as defined in the Logging TSS SHOULD be applied.

5.1.3 Highly Restricted

- Authentication SHOULD be carried out against a University IT Services operated Identity Provider which provides non-replayable authentication (e.g., Duo), in compliance with the Authentication TSS.
- Encryption SHOULD be applied in compliance with the Encryption TSS.
    - Highly Restricted Information SHOULD NOT be stored on devices which are "not trusted" (see 5.3).
- Logging and audit controls as defined in the Logging TSS SHOULD be applied.
- Highly Restricted Information SHOULD NOT be directly accessible from the public Internet.

5.2 Read Only ("Painted Screen")

Access to information in a read-only manner, where there is no scope to alter Information, and no content of the Information is stored in a persistent fashion on the client device MAY be permitted with no client side controls enforced provided that:

- The user Authentication is non-replayable (e.g., Duo); AND
- The volume of Information is small (e.g., an individual viewing their own Information); AND
- No residue of the information is left behind on the client device through mechanisms such as browser caches.

5.3 Trusted Devices

Devices are defined as follows:

- Managed
    - The device may be a member of Active Directory and managed by SCCM, or otherwise under the control and responsibility of the University (e.g., enrolled to inTune Mobile Device Management).
- Trusted
    - A subset of the managed estate, these devices will be provisioned with suitable digital certificates enabling identification of the device to the firewall. They are considered trustworthy for the purposes of access to resources within the Highly Restricted network zone.
    - Trusted mobile devices will be enrolled to the mobile device management (MDM) system and also possess the required digital certificate.

Devices that possess the required certificate will be considered trusted. All other devices will be classified as un-trusted, regardless of whether they are managed or not.

In order to become trusted a device SHOULD demonstrate compliance with the following TSS:

- Malware Defence
- Patching
- Cryptography
- Firewall
- Logging
- Any platform specific TSS that is applicable (e.g., Windows Workstation)

5.4 Deployment patterns

Deployment patterns SHOULD be aligned to the methodologies detailed in P00510 (IAM) and P00586 (NAAC)

5.5 Other Applicable Standards

The absence of a direct reference to another TSS in this document MUST NOT be construed to imply this set of controls is exhaustive; rather it is intended to provide a summary overview of the main baseline controls and deployment patterns/considerations. Full compliance with all standards is assured through following the Technical Risk Review (TRR) process (insert hyperlink here).

Supporting Policy, SOP and TSS can be found at
http://www.itservices.manchester.ac.uk/aboutus/policy

6 Compliance

Compliance with this Technical Security Standard will be verified during regular vulnerability scans, and audits and reviews by the Information Governance Office or equivalent, with the support of selected specialists.

Where particular controls cannot be implemented a formal security exception to this Standard MUST be agreed and approved with the HOIG.

Retrospective compliance MUST occur within six months of the approval of the Standard. If this is not possible because of clear business reasons, then a formal security exception to this Standard MUST be agreed and approved with the HOIG.

Non-compliant systems and applications are subject to disconnection from the University network.

7 Review

This Technical Security Standard will be reviewed at least every two years or when significant changes are required.

8 Contact list for queries related to this Technical Security Standard

Role	Name	Telephone	Email
TBC but in the meantime:			
Enterprise Architect	Matt Foster	-	matt.foster@manchester.ac.uk
IT Security Analyst	Lee Moffatt	0161 275 1258	lee.moffatt@manchester.ac.uk
Deputy Head of Information Governance	Barbara Frost	0161 275 2122	barbara.frost@manchester.ac.uk
Head of Information Governance	Tony Brown		Tony.Brown@manchester.ac.uk

If you are reading a printed version of this document you should check
http://documents.manchester.ac.uk/
to ensure you have the most up to date version

This document is owned by the Head of Strategy & Architecture, IT Services.

Version amendment history

Version	Date	Author	Reason for change
0.1	28-Nov-17	MPF	Initial Draft
0.9	13-Feb-18	MPF	Version for review by Security SIG
1.1	July 2018	MPF	Initial publication version