Technical Security Standard

Title:	**Minimum Controls TSS**		
Version:	**1.2**	**Effective Date**	**August 2021**
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 the University's online document system https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=37875

1 Introduction and purpose

This document is a Technical Security Standard and as such describes security control requirements which support compliance with legislative and regulatory requirements and University policies and procedures which are mandatory.

Detailed configuration and implementation requirements SHOULD be contained within operational procedure and guidelines documentation.

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.

2 Scope and definitions

This Standard defines the specification for the baseline requirements for minimum controls across all University IT systems, whether directly managed by University staff or the responsibility of a third-party partner or supplier and SHOULD be included as non-functional requirements for any new systems as appropriate.

The basic designs and principles described in this document provide minimum baseline protection for the University environment against potential unauthorised data modification and/or access. Third-party agreements may impose additional controls, and where these are more stringent, they take precedence over this Standard.

Where particular controls cannot be implemented, a formal security exception to this Standard MUST be agreed with and approved by the Head of Information Governance (HoIG). The Information Governance Exception Handling Standard Operating Procedure provides details on how to request an exception to the TSS.

In this document the terms **MUST** and **SHOULD** are used and when in upper case have the following meaning (as defined by Microformats.org https://microformats.org/wiki/rfc-2119):

- **MUST** means mandatory, is an absolute requirement.
- **MUST NOT** means forbidden – is an absolute prohibition.
- **SHOULD** and **SHOULD NOT** mean 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.

3 Roles and responsibilities

This document is intended to be read primarily by solution architects, project managers, members of the Security Operations Centre, partners and system administrators responsible for IT Services infrastructure and applications. Projects SHOULD specify non-functional requirements which meet the applicable Technical Security Standards.

The standards contained in this document will apply to all University systems whether directly managed by University staff or the responsibility of a third-party partner or supplier.

Staff must note that any breach of this Standard may be treated as misconduct under the University's relevant disciplinary procedures and could lead to disciplinary action and/or removal of IT access.

This Standard is owned by the Head of Information Governance.

4 Standard

4.1 General principles

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

4.2 Technical controls

4.2.1 Unrestricted

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

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.2.5 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)

4.2.6 Deployment patterns

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

4.2.7 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).

5 Monitoring compliance

Compliance with this Technical Security Standard will be verified during regular monitoring (such as vulnerability scans), audits and reviews by IT Services or equivalent, with the support of selected specialists, in order to provide evidence and assurance to the Information Governance Office.

Where particular controls cannot be implemented, a formal security exception to this Standard MUST be agreed with and approved by the HoIG. The Information Governance Exception Handling Standard Operating Procedure provides details on how to request an exception to the Standard.

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 exception MUST be agreed with and approved by the HoIG.

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

6 Review

This Technical Security Standard will be reviewed at least every two years (unless there is a specific requirement for more frequent reviews) or when significant changes are required.

7 Contact list for queries related to this Technical Security Standard

Role	Name	Telephone	Email
Enterprise Architect	Matt Foster	-	matt.foster@manchester.ac.uk
IT Security Analyst	Lee Moffatt	0161 275 1258	lee.moffatt@manchester.ac.uk
Head of Information Governance	Tony Brown	0161 306 2106	Tony.Brown@manchester.ac.uk

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
1.2	Aug 2021	BAF	Minor edits to bring in line with template approved by TDA – no change to standard

Document control box	
Title:	Minimum Controls TSS
Date approved:	August 2021
Approving body:	Technical Design Authority
Version:	1.2
Supersedes:	1.1
Previous review dates:	July 2018
Next review date:	August 2023
Related Statutes, Ordinances, General Regulations:	Statute XIII Part III re disciplinary procedures for staff: https://documents.manchester.ac.uk/display.aspx?DocID=16238 Ordinance XIV Intellectual Property Rights (IPR), Data Protection and the Use of Information Systems: https://documents.manchester.ac.uk/display.aspx?DocID=12072 University General Regulation XV Use of Information Systems; University General Regulation XVII Conduct and Discipline of Students – (I) re misuse of property and information systems: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=39973
Related policies:	Information Security Policy: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6525 Acceptable Use Policy – IT facilities and services: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16277
Related procedures:	Information Governance Exception Handling SOP: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=35328 Acquisition, development and maintenance of IT systems and/or services SOP: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16369 Acceptable Use SOP for staff: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16221 Acceptable Use SOP for students: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16220
Related guidance and or codes of practice:	IT Cyber Security: https://www.itservices.manchester.ac.uk/cybersecurity/
Related TSS Library standards	
Equality impact outcome:	N/A
TSS owner:	Head of Information Governance