# Technical Security Standard

|  |  |  |  |
|---|---|---|---|
| **Title:** | **Remote Access TSS** | | |
| **Version:** | **1.2** | **Effective Date** | **August 2021** |
| **Summary:** | **This Standard defines the security controls and processes associated with remote access.** | | |

**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=37874

## 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.

Networked IT systems are, by their nature, accessed from a variety of locations. The physical access controls associated with areas of the University campus, and equipment contained within them, are rarely present when access is carried out from another location. This standard details the compensating controls that reduce the associated risk.

## 2 Scope and definitions

This Standard defines the specification for the baseline requirements for remote access 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.

**Scope**

- Systems that provide onward network connectivity via VPN (or other) network tunnels.
- Proxy services, “Smart DNS” or similar technologies
- Systems that provide the capability to initiate new network connections and sessions, such as remote shell services (SSH, Remote Desktop etc.,)

## 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

- Access is considered to be “not remote” if the client device is connected to the University of Manchester wired Ethernet network OR is connected to the eduoram 802.11 Wi-Fi network as operated locally by the University; connecting to instances of eduroam at other instiutions is NOT local.
- All other client network access MUST be considered to be remote.
- This standard covers client based (individual user) Remote Access only, and not site-to-site connections to 3rd parties or remote University locations.

### 4.2 Technical controls

**4.2.1 Authentication**

Authentication of remote users SHOULD be in compliance with the Authentication Technical Security Standard.

**4.2.2 Logging**

Security events SHOULD be written to the security audit log and SHOULD be forwarded to the University Event and Incident Management platform in compliance with the Logging TSS. Specifically the following information SHOULD be included:

- Successful/unsuccessful login or logout, including username and timestamp.
- IP address of remote client.
- IP address(es) assigned to remote clients.
- Host or Service name recording the event

### 4.2.3 Network Protocols

Remote Access capability SHOULD only provide IP connectivity. Either IPv4 and/or IPv6 connectivty MAY be provided.

### 4.2.4 Cryptography

All Remote Access SHOULD be protected at the network transport layer by cryptography that is compliant with the Cryptography TSS.

### 4.2.5 Direct Internet Access

- Information and systems that are wholly classified as unrestricted MAY be accessed directly from the Internet.
- Information and systems that are routinely accessed by undergraduate students SHOULD be accessible directly from the Internet:
    - Such systems SHOULD be in compliance with the Authentication TSS.
    - Such systems MUST implement robust authorisation mechanisms to restrict the information available to that necessary to the individual student.
    - Remote Access to such systems by non undergraduates SHOULD be protected in line with the other controls detailed in this standard.
- Direct access to Restricted or Highly Restricted Information SHOULD be protected by a technology compliant with this standard.

### 4.2.6 Operational Responsibility

Systems providing Remote Access capabilities as defined in this standard SHOULD be operated by a function within IT Services, with clearly defined reporting lines to the Director of IT Services.

## 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 | 27-Sep17 | MPF | Intial Draft |
| 1.0 | 1-Dec-17 | MPF | Submitted for Peer Review |
| 1.1 | 22-Feb-18 | MPF | 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: | Remote Access TSS |
| Date approved: | August 2021 |
| Approving body: | Technical Design Authority |
| Version: | 1.2 |
| Supersedes: | 1.1 |
| Previous review dates: | February 2018 |
| Next review date: | August 2021 |
| Related Statutes, Ordinances, General Regulations: | Statute XIII Part III re disciplinary procedures for staff:<br>https://documents.manchester.ac.uk/display.aspx?DocID=16238<br>Ordinance XIV Intellectual Property Rights (IPR), Data Protection and the Use of Information Systems:<br>https://documents.manchester.ac.uk/display.aspx?DocID=12072<br>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:<br>https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=39973 |
| Related policies: | Information Security Policy<br>Record Management Policy<br>Data Protection Policy |
| Related procedures: | Information Governance Exception Handling SOP:<br>https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=35328<br>Acquisition, development and maintenance of IT systems and/or services SOP:<br>http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16369<br>Acceptable Use SOP for staff:<br>https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16221<br>Acceptable Use SOP for students:<br>https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16220 |
| Related guidance and or codes of practice: | IT Cyber Security:<br>www.manchester.ac.uk/cybersecurity |

| | |
|---|---|
| Related TSS Library standards | Cryptography, Authentication, Logging, Minimum Controls |
| Related information: | |
| Equality relevance outcome: | LOW |
| TSS owner: | Head of Information Governance |