MANCHESTER 1824
The University of Manchester

Technical Security Standard

Title:	**Remote Access TSS**		
Version:	**1.1**	**Effective Date**	**July 2018**
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 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

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.

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.

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.,)
-

5.1 General

- 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.

5.2 Authentication

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

5.3 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

5.4 Network Protocols

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

5.5 Cryptography

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

5.6 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.

5.6 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.

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
Information Security Manager	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	27-Sep17	MPF	Intial Draft
1.0	1-Dec-17	MPF	Submitted for Peer Review
1.1	July 2018	MPF	Publication version

Document control box	
Title:	Remote Access TSS
Date approved:	July 2018
Approving body:	IT Services – Strategy &Architecture
Version:	1.1
Supersedes:	All previous versions of this document.
Previous review dates:	Not applicable
Next review date:	July 2020
Related Statutes, Ordinances, General Regulations:	Statute XIII Part III re disciplinary procedures for staff; Ordinance XIV Intellectual Property Rights (IPR), Data Protection and the Use of Information Systems; University General Regulation XV Use of Information Systems; University General Regulation XVII Conduct and Discipline of Students – (l) re misuse of property and information systems
Related policies:	Information Security Policy Record Management Policy Data Protection Policy
Related procedures:	Acceptable Use of IT Facilities and Services - Standard Operating Procedure for Staff Acceptable Use of IT Facilities and Services - Standard Operating Procedure for Student Information Security Controls System Acquisition and Development Secure Configuration Authority to access and monitor University IT account holder communications and data - SOP
Related guidance and or codes of practice:	IT Cyber Security: www.manchester.ac.uk/cybersecurity
Related TSS Library standards	Cryptography, Authentication, Logging, Minimum Controls
Related information:	
Equality relevance outcome:	LOW
TSS owner:	IT Services, Security & Architecture
Lead contact:	Matt Foster