Technical Security Standard

Title:	**Cloud Computing TSS**		
Version:	**2.0**	**Effective Date:**	**November 2025**
Summary:	**This Standard defines the security controls relating to using cloud services.**		

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/display.aspx?DocID=37877

1 Introduction and Purpose

This document is a Technical Security Standard (TSS) 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.

Cloud computing services offer organisations access to a range of technologies and service models typically delivered over the internet.

By processing information in the cloud the University may encounter risks to data protection that it was previously unaware of. It is important that the university and its staff to take time to understand the risks that cloud computing presents to information management.

In particular for highly restricted classified information.

2 Scope and Definitions

This Standard defines the specification for the baseline requirements for cloud computing 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 when information is processed using web storage or services in terms of information security as well as Data Protection legislation. This Standard offers a set of questions and approaches the University should consider, in conjunction with a prospective cloud provider, in order to ensure that the processing of information done in the cloud complies with the GDPR and associated information, data protection and privacy legislation. Third-party agreements may impose additional controls, and where these are more stringent, they take precedence over this Standard.

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

This document defines the following terms: the terms **MUST**, **SHOULD** and **MAY** 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 Director of Information Governance if the requirement or prohibition is not met.
- **MAY** or the adjective "OPTIONAL", mean that an item is optional.

Cloud computing is defined as access to computing resources, on demand, via a network:

- **computing resources –** this can include storage, processing and software;
- **on demand –** the resources are available on a scalable and elastic basis. This typically involves the dynamic provision of virtualised resources. Users are often billed for the level of resource used; and
- **via a network –** the transit of data to and from the cloud provider. The transit of data may be over a local or private network or across the internet.

For further clarity the three main groups involved in the use and delivery of cloud services:

- **Cloud provider** – The organisation that owns and operates a cloud service (Note: More than one cloud provider may be involved in the supply chain of a single cloud service).
- **Cloud customer** – The organisation that commissions a cloud service for a particular purpose.
- **Cloud user** – The end user of a cloud service – for example a member of the public.

Cloud computing can be deployed using a number of different models:

- **Private cloud** – The cloud customer is the sole user of the cloud service. The underlying hardware may be managed and maintained by a cloud provider under an outsourcing contract. Access to the cloud service may be restricted to a local or wide area network.
- **Community cloud** – A group of cloud customers access the resources of the same cloud service. Typically the cloud customers will share specific requirements such as a need for legal compliance or high security which the cloud service provides. Access to the cloud service may be restricted to a wide area network.
- **Public cloud** – The infrastructure, platform or software is managed by the cloud provider and made available to the general public (cloud customers or cloud end-users). Access to the cloud service is likely to be over the public internet.
- **Hybrid cloud** – Describes a combination of private, community and public clouds. A cloud customer will segregate data and services across different cloud services, with access between them restricted depending on the type of data they contain.
- **Infrastructure as a Service (IaaS)** – An IaaS cloud offers access to the raw computing resources of a cloud service. Rather than purchasing hardware itself, the cloud customer purchases access to the cloud provider's hardware according to the capacity required.

- **Platform as a Service (PaaS)** – A PaaS cloud offers access to a computing platform which allows cloud customers to write applications to run within that platform, or another instance of it. The platform may in turn be hosted on a cloud IaaS.
- **Software as a Service (SaaS)** – A SaaS cloud offers access to a complete software application which the cloud user accesses through a web browser or other software. Accessing the software in this manner eliminates or reduces the need to install software on the client machine and allows the service to support a wider range of devices. The software may in turn be hosted on a cloud platform or infrastructure.

The scope of this Standard includes everyone who uses a cloud provider, has or is responsible for the procurement of a cloud storage or cloud service at the University of Manchester.

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. It should also be read by all University staff who intend to use cloud services, whether procured, commissioned or with no cost.

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.

Breach of this Standard may be treated as misconduct under the relevant University disciplinary procedures and could lead to disciplinary action and/or removal of IT access.

This Standard is owned by the Chief Information Security Officer.

4 Standard

4.1 General Principles

The following general principles SHOULD be followed in relation to access rights:

- Cloud services MUST be hosted in the UK or a country in receipt of an adequacy decision in accordance with UK GDPR, this includes EEA member countries. If the only solution is a country that hasn't been given adequacy, then there must be specific measures and safeguards in place to satisfy the requirements of UK GDPR.
- The University MUST identify all 3rd and 4th parties (i.e. the entire support chain) providing the service including (but not exclusively) support services, subcontractors, back-ups, recovery, datacentre mirroring and any others.
- The cloud service provider, will act appropriately in accordance with GDPR principles, in with their role as a data controller, joint data controller, processor etc, as defined by the services they are providing. The cloud service provider must report information security vulnerabilities and incidents or attacks to the University in a timely manner.
- Guaranteed data, application, service or process portability. (i.e., to another provider)

- The University SHOULD guarantee the deletion of data to agreed standards and specification when porting services, data etc. This includes the return of data on request in a usable format with decryption keys as necessary.
- The University SHOULD recognise all data controllers and data processors within the entire support chain, this includes 3rd and 4th parties to be reaffirmed in the associated contracts.
- The cloud service provider MUST be able to restore data (without alteration) from a back-up if it suffered a major data loss, particularly for the Universities' major information assets.
- The cloud service provider MUST have a Business Continuity plan in the event of DoS, Virus, failure, attacks, non-service, highjacked, social engineering etc. that will compromise Confidentiality, Integrity, Availability or Auditability.
- The cloud service provider MUST be able to communicate changes regarding the cloud service to the University service which may impact on the agreement, including breaches and changes of location.
- Highly restricted or very sensitive information and PII MUST follow the technical controls as cited in the Information security classification, ownership and secure information handling SOP .
- Secure service administration including formal change management processes.
- Provision of Audit information.
- Provide a list of the personal data to be held and how it will be processed in the cloud.
- Before acquiring a cloud service the University MUST perform an Information Governance Risk Review (IGRR) in line with the ADM SOP http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16369.

4.2 Technical Controls

- Appropriate security standards accreditation. (i.e., ISO27001, Cyber Essentials,etc)
- Secure interfaces and APIs Service and data protection at rest and during transmission must be in compliance with the Cryptography TSS.
- Secure interfaces and APIs, meet standards such as OWASP, no anonymous access, authenticated access only. (i.e., compliance with the Authentication TSS)
- Must be able to provide audit path and logs. (i.e., compliance with the Logging TSS)
- The University recognises standards set by the Cloud Security Alliance https://cloudsecurityalliance.org/ as best practice. Ideally service providers will be able to provide a minimum of CSA STAR level 2 attestation. If attestation is not available, the University MAY use the CCM controls framework in conjunction with University controls to benchmark the level of compliance.

5 Monitoring Compliance

Compliance with this Technical Security Standard will be verified during regular monitoring, technical audits and reviews by IT Services or equivalent. This is to provide evidence and assurance to the Information Governance Office.

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 Director of Information Governance.

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

6 Review

This Technical Security Standard will be reviewed at least annually (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	Email
Head of Security Architecture and Engineering	Phil Twiss	Philip.Twiss@manchester.ac.uk
IT Governance, Risk and Compliance Team	IT GRC	its-governance.risk.compliance@manchester.ac.uk

Version Amendment History

Version	Date	Author	Reason for change
1.5	April 2021	MV	1st principle amended in line with IGO advice/guidance
1.6	26/08/2021	BAF	Minor edits to bring in line with template approved by TDA – no change to standard
1.7	31/07/2025	Waterstons	External updates by Waterstons
2.0	28/11/2025	Damian Chim	Minor updates to formatting and wording Approval from ARB

Document Control Box	
Title:	Cloud Computing TSS
Date approved:	28/11/2025
Approving body:	Architecture Review Board
Version:	2.0
Supersedes:	1.6
Previous review date:	26/08/2021
Next review date:	28/11/2026
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 – (l) 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/display.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: https://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 Information security classification, ownership and secure information handling SOP: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971
Related guidance and or codes of practice:	IT Cyber Security: https://www.itservices.manchester.ac.uk/cybersecurity/
Related TSS Library standards:	Authentication TSS: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=33276
Related information:	
Equality impact outcome:	
TSS owner:	Chief Information Security Officer (CISO)