MANCHESTER 1824
The University of Manchester

Technical Security Standard

Title:	**Cloud Computing Technical Security Standard**		
Version:	**1.5**	**Effective Date:**	**April 2021**
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 at https://documents.manchester.ac.uk/display.aspx?DocID=37877 for latest version.

1 Introduction

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 higly restricted classified information.

2 Purpose

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.

3 Audience

This document is intended to be read primarily 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 cloud systems whether directly managed by University staff or the responsibility of an outsourced supplier.

The basic designs and principles described in this document provide minimum baseline protection for the University information when processed using web storage or services in terms of information security as well as Data Protection legislation.

Any exceptions to these standards MUST follow a formal exception processes with appropriate risk acceptance and approval. Legislative, Regulatory or 3rd party agreements may impose additional controls, which take precedence over this standard.

4 Definitions and scope

In this document the terms **MUST** and **SHOULD** are used and when in upper case have the following meaning

- **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.

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.

This document is owned by the Head of Strategy and Architecture.

5 Standard

5.1 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.
- Identification of 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.
- Clarification of role in relation to GDPR - data controller, joint data controller, processor.

- Communication plan for reporting information security vulnerability and incidents or attacks to the University in a timely manner
- Guaranteed data, application, service or process portability (i.e to another provider)
- Guaranteed deletion of data to agreed standards and specification when porting service, data etc. This include return of data on request in a usable format with decryption keys as necessary
- Data ownership: clear recognition of all data controllers, data processors, 3rd and 4th parties to be reaffirmed in the associated contracts
- Cloud provider to be able to restore data (without alteration) from a back-up if it suffered a major data loss, particulary for the University major information assets
- Cloud Service 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
- Mechanism in place so that the cloud provider can communicate changes to the cloud service which may impact on the agreement, including breaches and changes of location.
- Highly restricted information and PII MUST follows 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.
- Completion an Information Governance Risk Review (IGRR) in line with the ADM SOP http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16369.

5.2 Technical Controls

- Physical hardware separation from other customers data. Logical separation may be appropriate if this can be demonstrated to be robust by a vulnerability scan.
- Appropriate security standards accreditation. What security accreditation or quality standards do they hold? i.e ISO27001, Cyber Essentials etc.
- Secure interfaces and APIs Service and data protection at rest and during transmission (i.e 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 Universsity 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 attestatiuon is not available, the University may use the CCM controls framework in conjunction with University controls to benchmark the level of compliance.

6 Compliance

Compliance with this Technical Security Standard will be verified during 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 with and approved with by 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 exception MUST be agreed with and approved by 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
Head of Strategy and Architecture	Paul Dennington	65755	paul.dennington@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

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

Version amendment history

Version	Date	Author	Reason for change
1.0	13 Nov 17	MV	Initial draft
1.1	13 Dec- 17	MV	Updated
1.2	23 Feb 18	MF	Updates for Cyber Security SIG
1.3	30 Apr 18	MV	Inclusion of hardware seperqtion controls and reference to Cloud Security Alliance best practice
1.4	July 2018	MPF	Approved version for publication
1.5	April 2021	MV	1st principle amended in line with IGO advice/guidance

Document control box	
Title:	Cloud Computing TSS
Date approved:	
Approving body:	IT Services – Cyber Security SIG
Version:	1.5
Supersedes:	v1.4 of this document. "Cloud TSS"
Previous review dates:	Not applicable
Next review date:	April 2023
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 – (I) re misuse of property and information systems
Related policies:	Information Security Policy Acceptable Use Policy – IT facilities and services
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 Information security classification, ownership and secure information handling Standard Operating Procedure
Related guidance and or codes of practice:	IT Cyber Security: www.manchester.ac.uk/cybersecurity
Related TSS Library standards	Authentication Technical Security Standard
Related information:	
Equality relevance outcome:	LOW
TSS owner:	IT Services, Domain Architecture - Security
Lead contact:	Mike Vale