UNIVERSITY OF HULL

Cloud Security Policy

Document Classification:	Policy
Data Classification:	Public
Version Number:	1.0
Status:	Approved
Approved by (Board):	Information Governance Committee
Approval Date:	10 October 2019
Effective from:	10 October 2019
Next Review Date:	Annual
Document Authors:	Dan Chambers, Stewart Doyle
Document Owner:	Head of Service Assurance (Stewart Doyle)
Department/Contact:	help@hull.ac.uk
Summary:	Outlines University's expectations in relation to the security of cloud services used to process or store University data.
Scope:	Cloud hosted information services used within the University University members involved with the acquisition and/or operation of such services
Collaborative provision:	Not mandatory
Assessment: (where relevant)	Not applicable
Consultation: (where relevant)	Not applicable
Relevant legal frameworks:	
Related documents:	Information Governance and Assurance Policy (and sub-policies) Cloud Security Standards Cloud Security Survey Cloud Security Survey – Response Evaluation
Published locations:	www.hull.ac.uk/policies
Document Communication and Implementation Plan:	Available upon request.
All printed versions of this document are classified as uncontrolled.	

Cloud Security Policy

1. Introduction

When the University deploys a new information system, there is an increasing trend for it to do so in the cloud. Whilst there may be significant operational advantages to moving data processing functions to the cloud[1], failing to evaluate these services adequately may expose the University to unacceptable levels of risk. When the security of a cloud service upon which the University relies is breached, the University must be able to demonstrate that any risks to data were known and understood, and be certain that the measures the service provider had in place were reasonable and appropriate.

2. Purpose

This policy outlines how the University will assure cloud services acquired for the purpose of storing, or otherwise processing, University information in accordance with the provisions of the overarching Information Governance and Assurance Policy and its related sub-policies.

Compliance with this policy ensures that the University is able to demonstrate due diligence in regards to its selection, acquisition, and use of cloud solutions to conduct its operations.

3. Scope

This policy applies to all information services operated by, or on behalf of, the University where the underpinning infrastructure and/or applications associated to those services are hosted wholly or partly on the Internet.

This policy applies to all University members involved with or responsible for the acquisition of such services, and those assigned responsibility for their ongoing governance, management and operation.

4. Responsibilities

The Information Governance Committee will be responsible for approving this policy and ensuring that this policy and its implementation achieves the objectives of the University's Information Governance and Assurance policy.

Executive Senior Information Risk Owners (SIRO) are accountable for the use of cloud services within their remit, in accordance with the roles defined within the overarching Information Governance and Assurance Policy, and for ensuring compliance with this policy by appointed Information System Owners.

Executive SIROs will be required to provide explicit approval for the use of cloud services where the provider is unable to provide adequate levels of assurance in relation to the data being stored or processed.

Information System Owners will ensure that cloud services have been approved for use within their area by the relevant Executive SIRO, and ensure that they comply with this policy.

Information System Owners, or an appointed Information System Steward working on their behalf, will work with Data Protection, Information Security, and Legal specialists to ensure that the objectives of this, and related, policies are met.

[1] Cloud computing is a general term for anything that involves delivering hosted services over the Internet.

All University members are expected to abide by this policy. Any breaches, or deliberate non-compliance with this policy will be investigated and may be treated as misconduct under the appropriate disciplinary policy.

ICT Service Assurance, consulting with the relevant stakeholders, will be responsible for developing, maintaining and approving any documentation and procedures required to enact this policy including the Cloud Security Survey and Evaluation.

5. Policy

Individuals will not enter into legally binding contracts with cloud solution providers on behalf of the University without first ensuring that the requirements of this, and related, policies have been met.

Individuals must ensure that the overarching requirements of the Information Governance and Assurance policy, and its subsidiary policies, are met prior to adopting a cloud service into use.

Any cloud service used to store, or otherwise process University data must have its information security properties evaluated by suitably qualified individuals to determine the level of assurance the University has that security controls are present and effective. Evaluations will be conducted in accordance with the provisions of the Cloud Security Standards.

The level of assurance offered by cloud solution providers over whether adequate controls are present and effective must be commensurate with the risks associated to the information being stored, processed or transported by the service (**Table 1**). Exceptions should be formally approved by the relevant Executive SIRO.

Individuals should ensure that contracts (including Data Processing Agreements/Addendums) are reviewed in line with the expectations of the University Solicitor's Office.

Services in use will be evaluated when significant changes occur, or at contract renewal, whichever is the sooner.

Executive SIROs and the Information System Owners they appoint will be provided with the guidance and support necessary to assist them in satisfying the objectives of this and related policies.

Table 1: Assurance Level Matrix - Relationship between data classification and assurance levels.

	Classification			
	Public	**Internal**	**Restricted**	**Confidential**
	No Personal Data, or disclosure of Personal Data would be reasonably expected.	Contains Personal Data, but disclosure would not normally be reasonably be expected by the Subject.	Contains Personal Data, but disclosure would not be reasonably be expected by the Subject.	Contains Special Categories of Personal Data.
Low assurance Assertions or commitments only	**Appropriate**	**Inappropriate**	**Inappropriate**	**Inappropriate**
Medium assurance Assertions or commitments, evidenced in some way (e.g. contracts, historical data)	**Appropriate**	**Appropriate**	**Appropriate**	**Inappropriate**
High assurance Independently validated implementations (e.g. via third party audit)	**Appropriate**	**Appropriate**	**Appropriate**	**Appropriate**