



**UNIVERSITY
OF HULL**

Information Systems Security and Architecture Policy

Document Classification:	Policy
Data Classification:	Public
Version Number:	1.0
Status:	Approved
Approved by (Board):	Information Governance Committee
Approval Date:	19 April 2021
Effective from:	19 April 2021
Next Review Date:	Annual
Document Authors:	Steph Jones, Nigel Kavanagh, Dan Chambers
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 information systems and services used to process or store University data.
Scope:	Information systems and 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) Information Systems Security Assessment Information Systems Architecture Assessment Information Security Controls Policy
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.	

Information Systems Security and Architecture Policy

1. Introduction

- 1.1. Trying to get a clear picture of the risks the University takes when adopting new information systems can be a difficult task.
- 1.2. When the University decides to deploy a new information system, it must be certain that the solution both ensures appropriate security measures are in place and that it adheres to a set of architecture standards.
- 1.3. Information risks within all systems must be managed effectively.

2. Purpose

- 2.1. This policy outlines how the University will assure information systems implemented for the storing, processing, or transporting information assets, in accordance with the provisions of the overarching **Information Governance and Assurance Policy** and its related sub-policies.
- 2.2. Compliance with this policy ensures that the University is able to demonstrate due diligence in regards to its selection, acquisition, and use of information systems to conduct its operations.

3. Scope

- 3.1. This policy applies to all information services operated by, or on behalf of, the University. These include on-premise systems where their infrastructure reside in the University data centre, or cloud-hosted systems that are wholly or partly provisioned on the internet.
- 3.2. 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

- 4.1. 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 Information Governance and Assurance policy.
- 4.2. Executive Senior Information Risk Owners (SIRO) are accountable for the use of services within their area, 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.
- 4.3. Executive SIROs will be required to provide explicit approval for the use of services where the vendor is unable to provide adequate levels of assurance in relation to the system and how it stores or processes data.
- 4.4. Information System Owners will ensure that services have been approved for use within their area by the relevant Executive SIRO, and ensure that they comply with this policy.

- 4.5. 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.
- 4.6. 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.
- 4.7. 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 **Information Systems Security Assessment** and **Information Systems Architecture Assessment**.

5. Policy

- 5.1. Individuals will not enter into legally binding contracts with service providers on behalf of the University without first ensuring that the requirements of this, and related, policies have been met.
- 5.2. Individuals must ensure that the overarching requirements of the **Information Governance and Assurance Policy**, and its subsidiary policies, are met prior to adopting a service into use.
- 5.3. Any service used to store, process or transport University data must have its information security and architecture controls and standards evaluated by suitably qualified individuals to determine that they are present and effective. Evaluations will be conducted in accordance with the provisions of the **Information Systems Security Assessment** and **Information Systems Architecture Assessment**.
- 5.4. The assessments will cover both on-premise and cloud-hosted systems, reflecting their differing needs under the policy.
- 5.5. The level of assurance determined will be typically rated as 'low', 'medium', or 'high'.
- 5.6. The level of assurance offered by information system providers over whether adequate standards and 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**), unless exceptions are approved by the relevant Executive SIRO.
- 5.7. Individuals should ensure that contracts (including Data Processing Agreements/Addendums) are reviewed in line with the expectations of the University Solicitor's Office.
- 5.8. Services in use will be evaluated when significant changes occur, or at contract renewal, whichever is the sooner.
- 5.9. 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.

6. Assurance Matrix

6.1. Table 1 shows the relationship between data classification and assurance levels.

	Classification			
	Public No Personal Data, or disclosure of Personal Data would be reasonably expected.	Internal Contains Personal Data, but disclosure would not normally be reasonably be expected by the Subject.	Restricted Contains Personal Data, but disclosure would not be reasonably be expected by the Subject.	Confidential 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