UNIVERSITY OF HULL

Information Systems Assurance Policy

Classification:	Policy
Data Classification:	Public
Version Number:	2.0
Status:	Approved
Approved by (Board):	Information Governance Committee
Approval Date:	21 November 2023
Effective from:	21 November 2023
Next Review Date:	Annual
Document Authors:	IT Services – Cyber Security
Document Owner:	Director of Cyber Security
Department/Contact:	IT Services / support.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
Relevant CIS Control(s):	15.4 – 15.7
Relevant legal frameworks:	
Related documents:	Information Governance and Assurance Policy (and sub-policies) Information Systems Security and Architecture Assessment Information Security Controls Policy
Published locations:	Public website (www.hull.ac.uk)
Document Communication and Implementation Plan:	Available upon request.

1 Introduction

1.1 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 cyber security and architecture standards.

1.2 Information risks within all systems must be managed effectively.

2 Purpose

2.1 This policy outlines how the University will assure information systems/services implemented for the storing, processing, or transporting of 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 can demonstrate due diligence regarding 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-premises systems where their infrastructure resides 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 (IGC) 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 The Cyber Security team, 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 and 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 policy, the overarching requirements of the **Information Governance and Assurance Policy**, and its subsidiary policies, are met.

5.2 Any service used to store, process, or transport University data must have its information security and architecture controls and standards evaluated by Cyber Security to determine that they are present and effective. Evaluations will be conducted in accordance with the provisions of the **Information Systems Security and Architecture Assessment**.

5.3 The assessments will cover both on-premises and cloud-hosted systems.

5.4 The level of assurance determined will be typically rated as ‘low,’ ‘medium,’ or ‘high.’

5.5 The level of assurance, over whether adequate standards and controls are present and effective, must be proportionate 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.

5.6 Individuals should ensure that contracts (including Data Processing Agreements/Addendums) are reviewed.

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

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

5.9 Upon decommission of the service, executive SIROs, Information System Owners, and IT Services will collaborate to ensure that:

- User and/ or service accounts are deactivated, and any permissions are revoked;
- Data flows are terminated;
- IT hardware is decommissioned;
- Any stored data is securely disposed of.

6 Assurance Matrix

6.1 Table 1, below, 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**

7 Version History

Version	Date	Reviewed By
1.0	19 April 2021	Dan Chambers
2.0	20 September 2023	Hollie Huxstep