Information Systems Assurance Policy

Document Reference:	IT-POL-108
Document Classification:	Policy
Data Classification:	Public
Version number:	3.0
Relevant CIS Control(s):	15.4 – 15.7
Status:	Approved
Approved by (Board):	University Leadership Team
Approval date:	03 June 2025
Effective from:	03 June 2025
Review Frequency:	Annual
Next review date:	03 June 2026
Document author:	Cyber Security
Document owner:	Director of Technology
Contact:	IT Services
Collaborative provision:	No

State whether this document is applicable to the University's collaborative partners

Related documents:

University document: No

A University document applies across the institution, is approved by a committee of Council or Senate and is held in the University Policy Directory on SharePoint.

Published location: Information Governance and Assurance Policy (and sub-policies)
Information Systems Security and Architecture Assessment
Information Security Controls Policy

- The University has adopted the principles of Designing for Diverse Learners, and all policy documents should be written with reference to these principles. Further information is available at the Designing for diverse learners website.

- An Equality Impact Assessment (EIA) must be considered for all new and amended policies. Further information is available from the EIA section of SharePoint.

- This document is available in alternative formats from policy@hull.ac.uk.

Information Systems Assurance Policy

Table of Contents

Information Systems Assurance Policy

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 assess 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, and all policies referenced herein, shall apply to all members of the University community, including faculty, students, administrators, staff, alumni, authorized guests, delegates, and independent contractors (the “End user(s)” or “you”) who are involved with, or responsible for, the acquisition of such services and those assigned responsibility for their ongoing governance, management, and operation.

3.2 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.

4 Responsibilities

4.1 The Information Governance Committee (IGC) are 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 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, efficient, and meet the minimum cyber-security controls baseline.

5.3 Evaluations will be conducted in accordance with the provisions of the **Information Systems Security and Architecture Assessment**.

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

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

5.6 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 (see Table 1, below). Exceptions must be approved by the relevant Executive SIRO.

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

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, support, and training necessary to assist them in satisfying the objectives of this and related policies.

5.10 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 A grid-like structure that is used to classify different types of data according based on their importance, sensitivity, and confidentiality (risk level) and assign corresponding assurance levels to each level[1].

6.2 Table 1, below, shows the relationship between data classification and assurance levels.

[1] https://www.lepide.com/blog/what-is-a-data-classification-matrix/

	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 Responsible, Accountable, Consulted, and Informed (RACI) Matrix

7.1 A form of a responsibility assignment matrix (RAM) commonly used in project management[2]. A RACI matrix defines who is involved in the successful completion / implementation of a project, task, or in this case, a policy[3]. A brief definition of each role is given in the table below.

7.2 The table below outlines the roles that are involved in ensuring this policy is adhered to, enforced, and kept up to date.

	Definition	Role
Responsible (R)	Answerable for the correct completion of the task	IT Services
Accountable (A)	Delegates and must sign off (approve) the work that those *responsible* provide	Director of IT Operations
Consulted (C)	Provide input based on how this will impact their domain of expertise	Information Governance Committee
Informed (I)	Those who are kept up to date on progress	

8 Version Control

Version	Author	Date approved	Relevant section(s)
1.0	Dan Chambers	19 April 2021	All
2.0	Hollie Huxstep	20 September 2023	All
3.0	Hollie Felice, Carl McCabe, Nigel Kavanagh	08 May 2025	All

[2] https://www.forbes.com/uk/advisor/business/software/raci-chart/

[3] https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/