UNIVERSITY OF HULL

Information Security Controls Policy

Document Classification:	Policy
Data Classification:	Public
Version Number:	3.0
Status:	Approved
Approved by (Board):	Information Governance Committee
Approval Date:	11 October 2021
Effective from:	11 October 2021
Next Review Date:	Biennual
Document Authors:	Steph Jones
Document Owner:	Security and Architecture Manager, ICT (Steph Jones)
Department/Contact:	support.hull.ac.uk
Summary:	This policy sets out the high-level objectives that demonstrate the University's approach to information security controls. It provides the framework upon which a range of technical controls can be built and maintained.
Scope:	This policy applies to all University members
Collaborative provision:	Not mandatory
Assessment: (where relevant)	Not applicable
Consultation: (where relevant)	Not applicable
Relevant legal frameworks:	See relevant section of overarching Information Governance and Assurance Policy
Related documents:	Information Governance and Assurance Policy and sub-policies
Published locations:	Public website (www.hull.ac.uk)
Document Communication and Implementation Plan:	Available upon request.
All printed versions of this document are classified as uncontrolled.	

Information Security Controls Policy

1. Introduction

1.1. Information security controls are required to protect all aspects of the University information technology infrastructure and the data it stores. Controls ensure safeguards are applied to avoid, detect, counteract, or minimise security risks to information assets.

1.2. The University has approved the adoption and implementation of the CIS Controls[1], as published by the SANS Institute Center for Internet Security (CIS), as its security controls framework. The CIS Controls are a prioritised set of actions that collectively form a defence-in-depth set of best practices that mitigate the most common attacks against systems and networks.

2. Purpose

2.1. This policy establishes the University's commitment to implementing the CIS Controls as the basis for its information security management activities.

2.2. Successful implementation of this policy will ensure that the University is able to demonstrate that appropriate technical measures are in place to safeguard its information assets.

3. Scope

3.1. This policy applies to all ICT systems, infrastructure and data owned and/or managed by the University. This policy applies to University members involved in the management and/or implementation of information security controls.

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. ICT Security and Architecture and the Governance and Compliance Office will operate and maintain the overarching management framework (Information Security Management System (ISMS)) necessary to implement this policy effectively, and report on the progress of its implementation to IGC.

4.3. ICT Security and Architecture staff will be responsible for managing the security controls framework including identifying priorities of sub-controls to be implemented in proportion to risk, working with ICT staff primarily to agree appropriate implementation of sub-controls, and monitor their implementation and maturity.

4.4. University ICT staff will be responsible for the application of controls that are applied to ICT managed technologies.

4.5. Information System Owners and/or Stewards are expected to assist with, or may be entirely responsible for, the application of controls scoped to individual information systems. However, they must be made aware of their responsibilities by ICT Security and Architecture staff in order to comply.

[1] https://www.cisecurity.org/controls/