UNIVERSITY OF HULL

Information Security Controls Policy

Document Classification:	Policy
Data Classification:	Public
Version Number:	4.0
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:	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
Relevant CIS Control(s):	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.

1 Introduction

1.1 Information security controls are required to protect all aspects of the University's Information Technology (IT) 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.

1.3 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.

1.4 There are eighteen controls within version eight of the framework, and these controls are split into three different implementation groups (IGs) that define the cyber security maturity of an organisation. Appendix A provides a high-level overview of the security controls and IG definitions[2].

1.5 As a result of implementing and adhering to the CIS Controls framework, University policies will specify which controls are being met.

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 IT 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 Cyber Security 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 Periodic internal assessments will be conducted to review the University's adherence to the CIS Controls, as well as evaluating the cyber security maturity per control.

4.4 Cyber Security staff will be responsible for managing the security controls framework including identifying priorities of sub-controls to be implemented in proportion to risk. As well as working with IT Services staff primarily to agree appropriate implementation of sub-controls and monitor their implementation and maturity.

[1] https://www.cisecurity.org/controls
[2] https://www.cisecurity.org/insights/white-papers/cis-critical-security-controls-v8-poster

4.5 University IT Services staff will be responsible for the application of controls that are applied to IT managed technologies.

4.6 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 IT Services staff to comply.

5 Version History

Version	Date	Reviewed By
3.0	11 October 2021	Steph Jones
4.0	20 September 2023	Hollie Huxstep

6 Appendix A: CIS Controls Version 8 Overview

6.1 Implementation Groups Overview

6.2 List of CIS Security Controls

1) Inventory and Control of Enterprise Assets
2) Inventory and Control of Software Assets
3) Data Protection
4) Secure Configuration of Enterprise Assets and Software
5) Account Management
6) Access Control Management
7) Continuous Vulnerability Management
8) Audit Log Management
9) Email and Web Browser Protections
10) Malware Defenses
11) Data Recovery
12) Network Infrastructure Management
13) Network Monitoring and Defense
14) Security Awareness and Skills Training
15) Service Provider Management
16) Application Software Security
17) Incident Response Management
18) Penetration Testing