Information Security Controls Policy

Document Reference: IT-POL-109

Document Classification: Policy

Data Classification: Public

Version number: 5.0

Relevant CIS Control(s): Not Applicable

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: Information Governance and Assurance Policy and sub-policies

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: University Website

- 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 Security Controls Policy

Table of Contents

Information Security Controls Policy

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. Section 6 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.

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

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 use the University's IT Resources.

3.2 Specifically, university members involved in the management and/or implementation of information security controls.

3.3 The term "IT resources" refers to IT systems, infrastructure, and data owned and/or managed by the University.

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.

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 CIS Controls Version 8 Overview

5.1 The implementation groups are described as follows in the latest version guide[3]:

- **IG1** = An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information.
  Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.
- **IG2 (includes IG1)** = An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs.
  Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.
- **IG3 (includes IG1 and IG2)** = An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare.
  Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

5.2 The below list is of all eighteen CIS controls according to the eighth version:

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

[3] https://learn.cisecurity.org/cis-controls-download-v8

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

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

6.1 A form of a responsibility assignment matrix (RAM) commonly used in project management[4]. A RACI matrix defines who is involved in the successful completion / implementation of a project, task, or in this case, a policy[5]. A brief definition of each role is given in the table below.

6.2 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 Technology
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	University Leadership Team

7 Version Control

Version	Author	Date approved	Relevant section(s)
3.0	Steph Jones	11 October 2021	All
4.0	Hollie Huxstep	20 September 2023	All
5.0	Hollie Felice, Carl McCabe, Nigel Kavanagh	08 May 2025	All

[4] https://www.forbes.com/uk/advisor/business/software/raci-chart/
[5] https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/