UNIVERSITY OF HULL

Information Security Controls Policy

Document Classification:	Policy
Data Classification:	Public
Version Number:	2.0
Status:	Approved
Approved by (Board):	Information Governance Committee
Approval Date:	10 October 2019
Effective from:	10 October 2019
Next Review Date:	Annual
Document Authors:	Dan Chambers, Stewart Doyle
Document Owner:	Head of Service Assurance, ICT (Stewart Doyle)
Department/Contact:	help@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) and SharePoint (share.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

This policy is based on version 7 of the CIS Controls as published by the Center for Internet Security (CIS). 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. The CIS Controls are developed by a community of experts from a wide range of sectors including education, healthcare, government, and others.

2. Purpose

This policy establishes the University's commitment to the CIS Controls as the basis for its information security management activities. These principles will form the basis upon which the more detailed sub-controls will be based.

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

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

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's Information Governance and Assurance Policy.

ICT Service Assurance 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.

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

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 Service Assurance staff in order to comply.

5. Principles and implementation

The following principles and objectives map directly to the CIS Controls v7[1], and demonstrate the University's commitments to each of the key security control areas. Implementation will be handled via the University's ISMS as described in the overarching Information Governance and Assurance Policy.

5.1. Inventory and Control of Hardware Assets

All University owned hardware devices that connect to the network will be actively managed. Unmanaged and/or unauthorised devices may be limited in their ability to access University information and systems.

5.2. Inventory and Control of Software Assets

All software on the network will be actively managed. Unauthorised and/or unmanaged software that introduces information or security risks may be prevented from executing.

5.3. Continuous Vulnerability Management

A vulnerability management programme will be operated in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

5.4. Controlled Use of Administrative Privileges

Administrative privileges will be tightly controlled in order to limit the potential for an attacker to move laterally through networks and infrastructure.

5.5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

The security configuration of mobile devices, laptops, servers, and workstations will be actively managed using appropriate configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

5.6. Maintenance, Monitoring and Analysis of Audit Logs

Audit logs of events that could help detect, understand, or recover from an attack will be collected, managed and analysed.

5.7. Email and Web Browser Protections

The attack surface and the opportunities for attackers to manipulate human behaviour through their interaction with web browsers and email systems will be minimised through the implementation of controls that balance protection and productivity.

5.8. Malware Defences

Malware defences will be deployed using a layered approach in order to control the installation, spread and execution of malicious code.

5.9. Limitation and Control of Network Ports, Protocols and Services

The ongoing operational use of ports, protocols, and services on networked devices will be actively managed to minimise the number of vulnerabilities available to attackers.

[1] See https://www.cisecurity.org/controls/ for more information

5.10. Data Recovery Capabilities

The University will use proven processes and tools to properly back up critical information adopting proven methodologies that ensure timely recovery when required.

5.11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

The security configuration of network infrastructure devices will be actively managed using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

5.12. Boundary Defence

Controls may be implemented to detect, prevent or correct the flow of information between networks of different trust levels.

5.13. Data Protection

A number of tools and processes may be used to prevent or mitigate the effects of data exfiltration, and ensure the privacy and integrity of sensitive information.

5.14. Controlled Access Based on the Need to Know

A number of tools and processes will be used to control access to critical assets according to which persons, computers, and applications have an approved need to access those assets.

5.15. Wireless Access Control

The security of wireless networks, access points, and clients will be actively managed.

5.16. Account Monitoring and Control

The lifecycle of system and application accounts will be actively managed in order to minimise opportunity for attackers to leverage them.

5.17. Implement a Security Awareness and Training Program

The University will collectively develop and execute an integrated plan to assess and identify gaps in the specific knowledge, skills and abilities needed to support defence of the organisation, and remediate through policy, training and awareness programs.

5.18. Application Software Security

The security lifecycle of all in-house developed and acquired software will be managed in order to prevent, detect, and correct security weaknesses.

5.19. Incident Response Management

The University will collectively develop and implement an incident response infrastructure for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity and availability of the network and systems.

5.20. Penetration Tests and Red Team Exercises

The overall strength of the University's defences may be tested by simulating the objectives and actions of an attacker.