NORTH, WEST AND HEBRIDES
A TUATH, AN IAR IS INNSE GALL

Information Security Policy

POL-NWH-022

Lead Officer (Post):	ICT Services Manager
Responsible Office/ Department:	ICT
Responsible Committee:	Audit & Risk Management Committee
Review Officer (Post):	Head of Infrastructure
Date policy approved:	07.10.25
Date policy last reviewed and updated:	07.10.25
Date policy due for review:	07.10.28
UHI Single Policy / UHI NWH Policy:	UHI Single Policy
Public face / College internal facing only	Public facing
Date of Equality Impact Assessment:	23.09.25
Has a Data Privacy Impact Assessment been completed:	Will be completed by Compliance Team – Completed / Data Protection Officer has approved that no DPIA is required

Policy Summary

Overview	This overarching security policy is the leading policy in the ISO/IEC 27001:2005 documentation set and provides a statement of management commitment and direction in respect of Information Security and alignment with ISO/IEC 27001:2013.
Purpose	The policy outlines the management approach to information security and the principles that are applied in order to secure information. It also states roles and responsibilities for the various security related actions and activities.
Scope	It applies to all personnel whether staff, contractor, other third party or members of partnership organisations with access to the university partnerships' data or information systems.
Consultation	Policy developed by UHI ITDI and Information Security Officer in conjunction with UHI Academic Partners, HEFESTIS to be compliant with NCSC and IASME Cyber Essentials Cyber-Security requirements and recommendations.
Implementation and Monitoring	Implementation and monitoring ongoing through the use of active network and device scanning, with assigned teams at the local level responding to appropriate requirements or threats. Additional year-round compliance checks and actions to meet Cyber Essentials/CE+ audits twice-annually. Monthly Information Security Group consultations with HEFESTIS representatives to discuss active threats and actions. Quarterly Regional ICT Committee to discuss Strategic InfoSec concerns.
Risk Implications	Failure to implement and enact an Information Security policy risks endangering student, staff, and stakeholder personal and corporate data, leading to reputational damage, substantial fines from the ICO, and remedial costs.
Link with Strategy	ICT and Knowledge Management Strategy
Impact Assessment	Equality Impact Assessment: 23.09.25
	Privacy Impact Assessment:

1. Policy Statement

1.1
The university of the highlands and islands partnership computer and information systems underpin all of the university partnership's activities, and are essential to its research, teaching, commercial and administrative functions.
The university partnership recognises the need for its staff, students, visitors and contractors to have access to the information they require in order to carry out their work and recognises the role of information security in enabling this.
Security of information must therefore be an integral part of the university partnership's management structure in order to maintain continuity of its business, legal compliance and adhere to the university partnership's own regulations and policies.

1.2
The UHI University Court is ultimately responsible for this policy in relation to the university's data and for compliance within the university partnership and has delegated responsibility to the principal and vice chancellor; they will provide clear direction, visible support and promote information security through appropriate commitment and adequate resourcing.
The university secretary has senior management responsibility for information security, reporting to the university's executive and the risk and audit committee on relevant risks and issues. Localised replication of this policy for UHI North, West and Hebrides reflects changes in the policy where they have been agreed at the partnership level through interaction in steering groups like Regional ICT Committee, Records and Governance, and Information Security Group.

1.3
The respective academic partner is ultimately responsible for this policy in relation to their data and for compliance within the partner and has delegated responsibility to the partner senior management team; they will provide clear direction, visible support and promote information security through appropriate commitment and adequate resourcing.

1.4
The university's director of IT and digital infrastructure is responsible for ensuring that centrally managed information technology systems and services take account of relevant information security risks and that they are integrated into the information security system.
The university's information security officer is responsible for the maintenance of this policy and will review the policy annually and in line with changing factors including new and emergent threats to security and new operational requirements, and specifically to provide advice and guidance on the implementation of this policy.
The information security group comprising representatives from executive office and all academic partners is responsible for identifying and assessing security requirements and risks.

It is the responsibility of all line managers to implement this policy within their area of responsibility and to ensure that all staff for which they are responsible are:

1. Made fully aware of the policy;
2. Given appropriate support and resources to comply.

It is the responsibility of each member staff to adhere to this policy.

1.5
The university partnership is committed to protecting the security of its information and information systems. It is also committed to a policy of education, training and awareness for

information security and to ensure the continued business of the university partnership. It is the university partnership's policy that the information it manages shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to ensure appropriate legal, regulatory and contractual compliance.
To determine the appropriate level of security that should be applied to information systems, a process of risk assessment shall be carried out in order to define security requirements and identify the probability and impact of security breaches.
Specialist advice on information security shall be made available throughout the university partnership and advice can be sought via the service desk.
It is the university partnership's policy to report all information or information technology security incidents, or other suspected breaches of this policy.
All staff have a duty to report security incidents and data breaches to the service desk , and those that involve personal data to the relevant data protection officer.

1.6
Records of the number of security breaches and their type will be kept and reported on a regular basis to the university secretary.

1.7
Records of the number of security breaches and their type will be kept and reported on a regular basis to the relevant academic partner's senior management team and the information security officer.

Failure to comply with this policy that occurs as a result deliberate, malicious or negligent behaviour may result in disciplinary action.

2. Definitions

2.1
Cyber Essentials / Cyber Essentials PLUS:
A Scottish Government mandated internal and external audit conducted by UHI ICT teams at the Academic Partner level and UHI-Wide.

IASME
The external auditors selected by Scottish Government to provide audit and certification services for Cyber Essentials compliance.

NCSC
The National Cyber Security Centre – a UK Government branch dedicated to supporting Cyber Security for UK Private and Public sector organisations.

UHI ITDI
UHI Information Technology and Digital Infrastructure department, who liaise with the Information Security Officer and Academic Partner ICT Departments.

HEFESTIS
HE/FE Shared Technology and Information Services. HEFESTIS is a not-for-profit Shared Service organisation, jointly owned by member institutions across the Scottish University and College sectors

3. Purpose

3.1
This information security policy defines the framework within which information security will be managed across the university partnership and demonstrates management direction and support for information security throughout the university partnership. This policy is the primary policy under which all other technical and security related policies reside. Section 9 provides a list of all other policies and procedures that support this policy.

4 Scope

4.1
This policy is applicable to and will be communicated to all staff, students, visitors and contractors.
It covers but is not limited to, any systems or data attached to the university partnership's computer or telephone networks, any systems supplied by the university partnership, any communication sent to or from the university partnership and any data – which is owned by the university partnership or third party data held by the university partnership – held on systems external to the university partnership's network.

5 Exceptions

5.1
None, applies to all staff, students, and stakeholders whether they use ICT facilities or otherwise.

6 Notification

6.1
This policy has been approved by the university partnership committees and forms part of the university partnership's policies and procedures.

7 Roles and Responsibilities

7.1
The following individuals and groups are responsible for developing, implementing, and enforcing the policy:

UHI Information Security Officer
UHI Information Security Group – Comprises ICT managers and staff of the Academic Partnership, in collaboration with HEFESTIS representatives, and IASME auditors working in conjunction with the NCSC.

All staff, students, and stakeholders with access to UHI corporate data via electronic or other means are required to comply with the policy.

8 Legislative Framework

None

9 Related Policies, Procedures, Guidelines and Other Resources

9.1

The following policies support the implementation of this overarching information security policy:

NWH Acceptable use policy;
NWH Bring your own device policy;
NWH Computer operations policy;
Secure areas policy;
Security awareness policy;
Third party access policy;
Password control policy;
Incident management policy;
Protection against malicious software policy.

The following UHI procedures and guides support the implementation of this overarching security policy:

Summary of the Acceptable Use policy;
Definitions of User Types Guide;
Firewall Change Control Procedure;
Responsibilities of users with elevated rights;
Vulnerability Testing Procedures;

10 Version Control and Change History

Version	Date	Approved by	Amendment(s)	Author