UHI | INVERNESS

# Information Security Policy

# REFERENCE: PL/IT/2024/001

| | |
|---|---|
| Lead Officer | ICT Services Manager |
| Review Officer | Information Development Manager |
| Date first approved by BoM | 19 March 2015 |
| First Review Date | June 2017 |
| Date review approved by BoM | March 2024 |
| Next Review Date | March 2027 |
| Equality impact assessment | 26/01/24 |

| Reviewer | Date | Review Action/Impact |
|---|---|---|
| ICT Services Manager | 28.05.17 | Reviewed by BoM Audit Committee |
| ICT Services Manager | 24.09.20 | Updates to reflect changes in regulation and new Government guidelines |
| ICT Services Manager | 17.10.23 | Updates to officers responsible, changes in regulation and review of external guidelines |

## Contents

1. Policy Statement 3
2. Legislative framework/related policies 3
3. Scope 4
4. Information Management Security System (ISMS) 4
5. Information Security Incident Management 5
6. Responsibilities 5
7. Compliance 6
8. Monitoring 6
9. Review 7

## 1. Policy Statement

The purpose of the UHI Inverness Information Security Policy is to:

- Promote, develop, and maintain a consistent and secure approach to the handling, storing and processing of information.
- Ensure all staff, students and relevant third parties understand their responsibilities with regards to Information Security.
- Ensure the College Information assets and IT infrastructure are not misused.
- Ensure the College adheres to relevant Information Security legislation.

Failure to adequately secure information increases the risk of significant financial and reputational losses. This policy outlines the College's commitment and approach to Information Security as well as the roles and responsibilities required to support this.

## 2. Legislative framework/related policies

2.1. The legislative frameworks applying to this policy are.

- Data Protection Act 2018;
- UK General Data Protection Regulation
- Computer Misuse Act 1990;
- The Regulation of Investigatory Powers (Scotland) Act 2000;
- Freedom of Information (Scotland) Act 2002;
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

2.2. The related UHI Inverness policies/documents are.

- Data Protection Policy
- Records Management Policy
- UHI IS ICT Acceptable Use Policy
- Business Continuity Policy
- Risk Management Policy
- Staff Recruitment and Selection Policy
- Information Asset Register

2.3. External Standards relevant to this policy are:

- Information Security ISO/IEC 27001;
- Information Security ISO/IEC 27002;
- Records Management ISO 15489-1;
- The UCISA Information Security Toolkit.
- JANET Acceptable Use Policy.
- Scottish Government Cyber Resilience Strategy for Scotland
- Scottish Government Public Sector Cyber Resilience Framework
- National Cyber Security Centre: Cyber Essentials

## 3. Scope

3.1. The policy scope is to ensure that the three key principles of Information Security are upheld. That is:

- **Confidentiality**: Ensuring information assets are protected from unauthorised access or modification.
- **Integrity**: Ensuring information is accurate, complete, and is delivered by reliable systems.
- **Availability**: Ensuring information is accessible and useable when required for authorised use.

3.2. For the purpose of this policy, information includes data stored on computers (including mobile devices), transmitted across networks; printed out or written on paper; sent out by fax; stored on disk or tape; and, spoken in conversation or over the telephone, including voicemail recordings.

3.3. As such, all information that is created, processed, stored. or transmitted physically or electronically as part of UHI Inverness' educational and related business activities is an asset of the organisation and, therefore, should be appropriately protected.

## 4. Information Security Management System (ISMS)

4.1. This policy defines an approach to Information security based on implementing and maintaining a fit for purpose set of controls, including policies, procedures, training, software, and hardware functions that formulate the Inverness College Information Security Management System (ISMS),

4.2. The ISMS is integrated with the College's processes and management structure and as defined in ISO 27000, appropriate for the educational purpose of the College.

4.3. The ISMS facilitates a risk-based approach to Information Security. For example, the management of personal data, such as student / staff records or financial records, would be different to that of public facing website or course materials.

4.4 The ISMS allows the College to:

- Understand how its information assets are protected against threats, both electronic and physical.
- Maintain a framework for identifying and assessing security risks, as well as applying applicable controls to address these.
- Classify information to indicate its sensitivity and importance to the College.
- Maintain key Information System operations even in the event of disaster, such as floods or IT outages.
- Maintain a programme, including training, to promote Information

Security awareness across the College.
- Ensure breaches of information security are reported, investigated and appropriate action is taken.

4.5 In addition to the legislative framework and College policies, referred to above, a number of other information security polices and guidelines will from part of the ISMS.

## 5. Information Security Incident Management

5.1. Any member of staff, student or researcher aware of any information security incident should report it to the College Data Controller (data.controller.ic@uhi.ac.uk). The Information Security Incident Management Procedure details how such events are handled and how lessons learnt are taken forward.

## 6. Responsibilities

6.1. The **Board of Management** are responsible for approval of the Information Security Policy.

6.2. The **Executive Management Team** is responsible for providing leadership and commitment to the application of Information Security, including ongoing review of the Information Security Policy.

6.3. The **Vice Principal - Student Experience and Quality** has operational responsibility for Information Security.

6.4. The **ICT Services Manager** is responsible for:
- Reviewing and maintaining the Information Security policy and updating the ISMS to address new threats, legislation and operational requirements of the College.
- Provision of specialist advice on matters of Information Security.
- Identifying and addressing risks to information systems.
- Ensuring that new systems or changes made to the College's ICT do not compromise the security of the existing infrastructure.

6.5. The **Information Development Manager** is responsible for:
- The classification scheme for information based on its importance to the College.
- Providing advice and guidance to staff with regard to record keeping, storage and destruction of documents.

6.6. The **MIS Manager** is responsible for:

- Ensuring business processes associated with the collation, interpretation and reporting of information across the College are robust, auditable and implemented by all staff.

6.7. The **Estates and Campus Services Manager** is responsible for:

- Ensuring the physical and environmental security of the Inverness College premises.
- Ensuring the secure storage and processing of confidential waste.

6.8. **Information Asset Owners** are responsible for:

- Determining and reviewing the level of access to be granted to staff, students and third parties to ensure the information they manage is appropriately accessible and secure.

6.9. All **Managers** are responsible for:

- Ensuring their staff are aware of their security responsibilities.
- Ensuring their staff have appropriate training for the systems and information they are using or processing.
- Ensuring staff complete the mandatory online module for data protection and information security annually.

6.10. All **Staff** should be aware that Information Security is their responsibility and should be considered as part of everyday working practice. As such, they are responsible for are responsible for:

- Ensuring they comply with the ICT Acceptable Use Policy.
- Reporting any security incidents as and when they are aware of them.
- Undertake mandatory information security and data protection training as and when required by the College.

6.11 All **Students** must abide by the UHI Acceptable Use Policy which documents how to use the College's ICT appropriately.

## 7. Compliance

7.1. This policy applies to all staff, students, contractors, third parties and partner organisations. Non-compliance should be raised as security incident to the ICT Services Helpdesk.

## 8. Monitoring

8.1. The effectiveness of the Information Security Policy and Information Security Management System requires periodic and event-based monitoring. Any organisational changes to the College structure, legislative change or major ICT changes may require review of this policy and others.

8.2. In addition, the evaluation of new Information Security risks may result in actions to add new, amend or delete existing controls. For example, a

review of the Physical Security would be required on the College opening a new campus.

8.3. Each college policy will be monitored, and its implementation evaluated. Appropriate procedures for monitoring and evaluation are the responsibility of the lead officer. These procedures will be subject to audit.

8.4. The number of Information Security incidents raised is recorded in a Data Breach Log by the Data Controller. The Data Controller reports statistical data and lessons learned to the senior management team and the Board of Management.

## 9. Review

9.1. The Information Security Policy shall be reviewed annually by the ICT Services Manager and presented for approval to the Board of Management or other designated committee every 3 years.