Institute of Technology, Sligo

Information Security Policy

Version 0.2

Document Location

The document is held on the Institute's Staff Portal here.

Revision History

Date of this revision: 28.03.16	Date of next review:

Version Number/Revision Number	Revision Date	Summary of Changes
0.1	25.11.14	
0.2	28.03.16	Replaced Head of Development and Business Operations with Secretary/Financial Controller or nominated member of the Executive Committee

Consultation History

Version Number/Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes

Approval

This document requires the following approvals:

Name	Title	Date
	Governing Body	28.09.16

This policy shall be reviewed and updated annually.

Table of Contents

1. PURPOSE

IT Sligo's information systems underpin all of the Institute's activities, and are essential to its teaching, learning, research and administrative functions. Security of information must therefore be an integral part of the Institute's operation and structure to ensure continuity of business, legal compliance and to protect IT Sligo from financial and reputational loss.

The purpose of this document is to set direction for information security management within IT Sligo. The policy sets out the overall approach to information security and provides a security model aimed at:

- Implementing best practices to protect information assets from unauthorized use, disclosure, modification, damage or loss.
- Protecting the work and study environment of staff and students and the good name and reputation of IT Sligo.

IT Sligo's information security policy should be read in conjunction with relevant standards, procedures and guidelines which support the implementation of this policy (Refer to Section 5).

2. DEFINITONS

Information Security – According to the ISO 27002 standard defines information security as the preservation of confidentiality, integrity and availability of information.

Confidentiality – Confidentiality restricts information access to authorised users.

Integrity – Integrity protects the accuracy and completeness of information through the controlling of information modifications.

Availability – Availability ensures the information is accessible when needed.

Information Asset –The ISO 27002 Standard defines an asset as anything that has a value to an organisation. Information has value and is classified as an asset. Information refers to data that is processed but also encompasses unprocessed data that is stored on IT Sligo's Information Technology (IT) resources.

Content - Content is information with relevant metadata that has a specific use or is used for a particular business purpose.

Records – ISO 15489 defines records as "information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.

Information Technology (IT) Resource – All IT systems owned, held under licence or otherwise controlled by IT Sligo including but without limitation to:

- Workstations including desktop PCs, laptops and netbooks;
- Servers;
- Network technologies such as routers (WAN, LAN and wireless) and associated media and systems;

- Printers;
- Phones, Smart Phones, tablets and other portable ICT devices;
- USB and all portable memory devices;
- All other media and devices provided by IT Sligo;
- All other media and devices used to access IT Sligo Information Assets.

Sensitive Personal Data – According to the Data Protection Acts 1988-2003, personal data is data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into the possession of a data controller. IT Sligo is both the data controller and data processer in relation to student and staff data.

3. ROLES AND RESPONSIBILITES

The following roles and responsibilities apply in relation to this Policy:

Governing Body:

- To review and approve the policy on a periodic basis.

Secretary/Financial Controller or nominated member of the Executive Committee:

- To ensure the Policy is reviewed and approved by the Governing Body.
- To consult as appropriate with other members of the Executive and Management Teams.
- To liaise with Human Resources (HR) or Registrar's Office on information received in relation to potential breaches of the Policy.
- To ensure the appropriate standards and procedures are in place to support the Policy.

IT Manager:

- To define and implement standards and procedures which enforce the Policy.
- To oversee, in conjunction with Data Owners, compliance with the policy and supporting standards and procedures.
- To inform the Secretary/Financial Controller or nominated member of the Executive Committee of suspected non-compliance and/or suspected breaches of the policy and supporting standards and procedures.

HR Office and Registrar's Office

- To follow relevant and agreed disciplinary procedures when HR or the Registrar's Office is informed of a potential breach of the Policy (Refer to Section 7).
- To manage the disciplinary process.

Staff/Students/External Parties:

- To adhere to policy statements in this document.

- To report suspected breaches of policy to their Head of Department or the IT Manager.

If you have any queries on the contents of this Policy, please contact the Secretary/Financial Controller or the IT Manager.

4. SCOPE

This Information Security Policy covers security of:

- IT Sligo Information Assets
- IT Sligo IT Resources

This policy applies, but is not limited to, the following IT Sligo related groups:

- IT Sligo staff
- IT Sligo students
- IT Sligo external parties

Based on the definition of Information Security in section 2, this policy outlines key policy statements relating to these areas.

5. SUPPORTING DOCUMENTS

- IT Sligo's Acceptable Usage Policy
- IT Sligo Password Standard
- IT Sligo Change Control Procedure
- IT Sligo Disaster Recovery Plan

The above list is not exhaustive and other IT Sligo documents may also be relevant.

6. POLICY

CONFIDENTIALITY

IT Sligo and all staff, students, and external parties of the Institute community are obligated to respect the rights of individuals and to protect confidential data.

All IT Sligo information is to be treated as confidential unless otherwise indicated. When data is classified as confidential data, appropriate access and security controls are applied in transmission and storage. Confidential data is not to be transmitted without adequate precautions being taken to ensure that only the intended recipient can access the data.

Access to information is granted on a needs only basis; IT Sligo staff are granted specific access to allow them to carry out their job functions.

All information is stored in a secure manner; this may require physical and logical restrictions. At a minimum, logical security includes the use of unique identifiers and passwords which are sufficiently complex where staff, students and external parties operate in accordance with IT Sligo Password Standard.

All hardware used for the storage of the IT Sligo's data is to be purged of data and securely destroyed once it is no longer to be used.

When tapes and other secondary storage devices reach the end of their useful life they are to be purged of the IT Sligo's data and securely destroyed.

INTEGRITY

Access to amend information and/or access to systems which process and record this information is restricted to authorised personnel.

System changes should be completed in accordance with the IT Sligo Change Management procedure with which all IT Sligo personnel should be familiar.

An appropriate audit trail including database logs of the creation, amendment and deletion of IT Sligo data and/or systems is maintained by the IT Sligo and/or nominated external parties. This is particularly important in relation to the following:

- Data including details on staff, students and suppliers;
- Data including inward fee payments, outward supplier payments, and payroll transactions;
- IT Sligo resource usage data.
- IT Sligo data which may reside outside main IT Sligo system(s).

AVAILABILITY

To ensure that IT Sligo data and resources are available when required, three key layers of control are employed:

- Prevention of data loss through data back-ups
- Prevention of system downtime and/or unauthorised data access and amendment through anti-virus protection
- Ability to respond to events which prevent data/system access through Disaster Recovery Planning (DRP)

7. POLICY AWARENESS AND DISTRIBUTION

New Staff and Students

This Policy will be available from IT Services on request. It will also be published on the IT Security web site. New staff and students will be notified of the relevant policy documents when they initially request access to the Institute network.

Existing Staff, Students, Authorised Third Parties and Contractors

Existing staff and students of the Institute, authorised third parties and contractors given access to the Institute network will be advised of the existence of this policy statement. They will also be advised of the availability of the associated policies and procedures which are published on the Institute website.

Logon Banner

Users logging onto the Institute Domain will be reminded of their obligations regarding compliance with the IT Security Policy via a Logon banner.

Updates

Updates to Policies and procedures will be made periodically and will be posted to the IT Services webpage.

8. MONITORING

IT Sligo reserves the right to monitor all IT Sligo information resources and IT Sligo data. Any monitoring of IT Sligo data and/or IT Sligo information resources may be random or selective depending on circumstances at that time.

IT Sligo reserve the right to log any required IT Sligo data concerning systems access, including data relating to unauthorised access attempts which may warrant investigation.

IT Sligo may also log all changes made to IT Sligo systems and applications.

9. VIOLATION OF POLICY

Contravention of any of the above policy will lead to the removal of IT Sligo resource privileges and can lead to disciplinary action in accordance with the IT Sligo disciplinary procedures.