Ollscoil
Teicneolaíochta
an Atlantaigh

Atlantic
Technological
University

Information Security Policy

Version 1.0

Revision History:

Date of this revision: 9th May 2022	**Date of next review:** May 2023

Version Number/ Revision Number	Revision Date	Summary of Changes	Changes marked
1.0	9th May 2022	New Policy	

Consultation History:

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

Approval:

This document requires the following approvals:

Version	Approved By:	Date
1.0	ATU Governing Body	9th May 2022

Quality Assurance:

Date Approved: 9th May 2022	Date Policy to take effect: 9th May 2022	Date Policy to be Reviewed: 9th May 2023
Written by:	IT PSC	
Approved by:	VP Finance and Corporate Services	
Approving Authority:	ATU Governing Body	
Head of Function responsible:	President ATU and President's Nominee	
Reference Documents:	Acceptable Usage Policies of GMIT, LYIT, IT Sligo, and ATU	

Document Location:

Website – Policies and Procedures	X
Website – Staff Hub	X
Website – Student Hub	X
Other: - Internal Use Only	X

Electronic copy stored on;

ATU website (www.atu.ie)
ATU Donegal website (www.lyit.ie), staff portal and student portal
ATU Sligo website (www.itsligo.ie), staff portal and student portal
ATU Galway Mayo website (www.gmit.ie), staff portal and student portal

This Policy was approved by the Governing Body on 9th May 2022. It shall be reviewed and, as necessary, amended by the University annually. All amendments shall be recorded on the revision history section above

Table of Contents

1. PURPOSE

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

The purpose of this document is to set direction for information security management within ATU. 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 ATU.

ATU 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

Regional Campuses - Regional campuses refer to Donegal, Sligo and Galway/Mayo campuses within the ATU.

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 ATU 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 organization 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 ATU including but without limitation to:

- Workstations including desktop PCs and laptops;
- 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 ATU;
- All other media and devices used to access ATU Information Assets.

Personal Data - personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Personal Data - Sensitive Personal Data (or Special Categories of Personal Data) relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life, criminal convictions or the alleged commission of an offence; trade union membership.

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

Senior Management Team:

- 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 Data Protection Officer 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 Managers:

- 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 Data Protection Officer and relevant senior management team of suspected non-compliance and/or suspected breaches of the policy and supporting standards and procedures.

HR Office and Office of the VP Academic Affairs and Registrar:

- To follow relevant and agreed disciplinary procedures when HR or the Office of the VP Academic Affairs and Registrar / senior management team 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 and/or Data Protection Officer.

4. SCOPE

This Information Security Policy covers security of:

- ATU Information Assets;
- ATU IT Resources.

This policy applies but is not limited to the following, ATU related groups as defined in Section 3.0 of the IT Documentation Framework:

- ATU staff;
- ATU students;
- ATU 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

- ATU Acceptable Usage policy;
- Existing Regional Campuses Policies, Procedures & standards.

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

6. CONFIDENTIALITY

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

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 need only basis; ATU 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 regional campus password standard.

All hardware used for the storage of ATU 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 ATU Data and securely destroyed.

7. 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 local change management procedure with which all ATU personnel should be familiar.

An appropriate audit trail including database logs of the creation, amendment and deletion of ATU data and/or systems is maintained by ATU. 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;
- ATU resource usage data;
- ATU data which may reside outside main ATU system(s).[1]

8. AVAILABILITY

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

- Prevention of data loss through data back-ups or redundancy.
- 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).

9. MONITORING

ATU reserve the right to monitor all ATU IT resources, information assets, content and data at all times.

Any monitoring of ATU data and/or ATU information resources is to ensure the secure, efficient and effective operations. The monitoring is non-intrusive and does not involve access or reading of content.

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

ATU may also log all changes made to ATU systems and applications.

10. VIOLATION OF POLICY

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

[1] This could include data which resides on external systems or data that resides on internal such as Excel Spreadsheets, local desktop databases, etc.