Ollscoil
Teicneolaíochta
an Atlantaigh

Atlantic
Technological
University

Third Party ICT Access Policy
Version 1.0

Revision History:

Version Number/ Revision Number	1.0
Date of this revision:	24 June 2024
Date of next review:	01 June 2026
Revision Date	24 June 2024
Summary of Changes	New Policy
Changes Marked	Yes/No

Consultation History:

Number/ Revision Number	1.0
Consultation Date	11 October 2023
Names of Parties in Consultation	IT Governance Committee
Summary of Changes	Reviewed new policy

Number/ Revision Number	1.0
Consultation Date	12 January 2024
Names of Parties in Consultation	UPT
Summary of Changes	Reviewed and approved by UPT

Number/ Revision Number	1.0
Consultation Date	24 January 2024
Names of Parties in Consultation	TUI and PMSS Unions
Summary of Changes	Reviewed by Unions

Approval:

This document requires the following approvals:

Version:	1.0
Approved By:	ATU Governing Body
Date:	24 June 2024

Quality Assurance:

Date Approved	24 June 2024
Date Policy to take effect:	01 September 2024
Date Policy to be reviewed:	01 June 2026
Written by:	IT PSC
Approved by:	IT Governance Committee
Approving Authority	ATU Governing Body
Head of Function responsible	President ATU and President's Nominee
Reference Documents:	Information Security Policy

Document Location:

Website – Policies and Procedures	Yes
Website – Staff Hub	Yes
Website – Student Hub	No
Other: - Internal Use Only	No

This Policy was approved by the Approving Authority on **24 June 2024**. It shall be reviewed and, as necessary, amended by the University annually or at such time as is deemed as necessary. All amendments shall be recorded on the revision history section above.

Note: Prior to publication and dissemination of policies and procedures, documents must be reviewed for accessibility as part the University's commitment to Equality, Diversity, and Inclusion (EDI). Further advice on accessibility can be obtained from the EDI Team.

Table of Contents

1. Overview / Introduction

This policy outlines the minimum-security requirement for third parties accessing Atlantic Technological University (ATU) information technology (IT) resources must comply with, to ensure the protection of the University systems and data.

2. Purpose of Policy

The purpose of this policy is to outline the minimum level of security controls that must be established before granting third-party access to ATU IT resources. The policy is to minimize the risk of a security breach which could result in adverse repercussions for ATU, including damage to its reputation, legal implications, and financial consequences.

3. Definitions

Third Parties: Third Parties are defined as any individual consultant, contractor, subcontractor, vendor, or agent not registered as an ATU employee, or student but who will require access to specific elements of ATU ICT infrastructure, systems and/or data stored on ATU systems.

Third Party Access: Third party access is defined as all physical or remote access to ATU ICT infrastructure, systems, or data for the express purpose of providing goods or services to the university.

IT Resources: IT Resources refers to ATU's digital information and data. These resources encompass hardware, software, applications, databases, network equipment, cloud services, and other related technologies that collectively enable the functioning of information technology systems and services.

ATU System/Data Owners: ATU system/Data owners refers to an individual or functional\academic department that is responsible for the overall management and control of

specific information system or a set of data within the ATU.

Authorised Personnel: The approver of the third-party account. By approving the account they take responsibility for ensuring the third party is aware of their responsibilities in respect to adherence to all applicable ATU policies.

4. Scope

This policy applies to:

- ATU staff who are responsible for managing or engaging with a third party who is providing goods or services to the University and need access to the IT resources.
- Third parties who are contracted by the University to provide goods or services and require either physical or remote access to the University IT resources.

5. Roles and Responsibilities

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

Governing Body:

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

IT Governance Committee

- To ensure policy is reviewed periodically and approved by the Governing Body.

ATU System/Data Owners

- To ensure that appropriate contracts and agreements are in place, and to schedule periodic reviews of third-party compliance with this policy. Also, to ensure where relevant that third parties are familiar with this policy.

Third parties

- To ensure that they are familiar with the content of this policy, before signing a third-party access agreement with ATU.

Information Solutions and Services Department

- To assist ATU system and data owners in ensuring that appropriate oversight is in place with relevant third parties.
- To ensure that security of ATU IT resources is not compromised because of providing access to a third party.

6. Policy Statement

This policy aims to ensure the security, integrity, and confidentially of university data and systems while facilitating necessary access for authorised third parties.

- A Third-party IT Access agreement must be signed by an authorised representative of the third party, and a member of ATU IT management team. Such agreement must include details on:
    - The parties to the agreement, including any relevant sub-contractors.
    - The effective start and end dates for the services being provided.
    - The functions/services being provided.
    - The right of ATU to monitor all access by the third party, and to audit compliance of the third party with this policy.
- Third party access to ATU systems or information resources must be approved by the Data Owner and a member of ATU IT management team.
- Third party access may only be used for the business purposes that it has been

granted for.

- Third party remote access to the ATU IT resources must use a remote access technology approved by Information and Solution Services Department.
- All third-party remote access connections must use encrypted communication and include multi-factor authentication.
- Third-party remote access to IT resources shall not be left unattended.
- Third-party remote access accounts will be limited for duration of the task or project.
- Isolated third-party access on a non-routable VLAN where third party access is required to manage onsite equipment, allowing network access only to the specific equipment involved. Implement separate Internet IP address and appropriate firewalls rules to restrict access to only the required ports and services.
- The issuing of access credentials must be done in a secure fashion. Username and password should not be communicated in the same written communication. Passwords should never be sent unencrypted.
- Third parties are responsible for ensuring that only nominated employees have access to approved IT resources.
- All third-party access must be uniquely identifiable, and passwords used must comply with ATU Password standard. Generic accounts are not allowed.
- Usernames, passwords, and any other credentials used for third party access must not be shared.
- Third parties will be held responsible for all activities performed on the ATU IT resources while logged in under their assigned username and password, in accordance with all applicable IT policies.
- ATU data must not be copied, divulged, or distributed by third parties without prior

written approval by authorised personnel in ATU.

- ATU data must never be updated by third parties without the express permission of the relevant ATU data owner, and a record must be made of all changes.
- Any changes that impact service delivery to the University must obtain prior approval in ATU change management process.
- Access to a University system will only be provided for the minimal period necessary, and with the minimum level access required to complete the task. Access will never be left open indefinitely and will be closed without notice following the agree period.
- All requests for amendments to third party access privileges must be formally approved by the data\system owners.
- Where third parties are connecting to ATU IT resources from a remote location, they must attest to having appropriate physical, and IT based security controls are in place. This will include physical locks, automated key cards, logical controls, and access logging.
- Third parties must attest to having appropriate information security and practices in place, and ensure any devices or software used to access ATU IT resources are fully up to date with virus protection, personal firewalls, and security updates. The third party will be held responsible for all disruption or damaged caused to ATU IT resources which is traced back to infected device or software.
- Third parties must attest to committing to ensuring that computer devices connected to ATU network are not connected to any other network at the same time, with exception of networks under the complete control of the third party.
- Under no circumstances should ATU data be stored on mobile devices, in personal backup or on removable storage devices by the third party.

- While onsite third parties must comply with all relevant ATU physical access controls, rules, and regulation.

- Third parties must inform a member of ATU IT management team immediately of any suspected or actual security or data breach.

- All relevant data protection, legal and regulatory requirements must be compiled with.

7. Policy Monitoring\ Compliance and Review

ATU reserves the right to:

- Monitor all third-party activities while connected (local and remote) to ATU IT resources.

- Audit contractual responsibilities and have those audits carried out by ATU or approved third party.

- Revoke the third parties access privileges at any time.

Any violation of this agreement by third parties, may lead to termination of access agreement to ATU IT resources.

Exceptions to this policy will require approval by the Vice President for Information Solutions and Services.

8. Supporting Documents

Below is a list of a suite of policies and procedures that may be used in conjunction with this policy.

- Information Security Policy
- Acceptable Usage Policy
- Password Standard

9. Appendix A – Third Party Access Agreement

The purpose of this agreement is to delineate the specific terms and conditions governing access to and use of ATU IT resources by a third party. This agreement is entered into by and between the third party and ATU, with the understanding that all parties involved will ensure compliance with the Third-Party Access Policy and associated policies as outlined in section 8.

This agreement, made between Atlantic Technological University (ATU) and _____ shall take effect on: _____ and shall expire on _____

Signed for and on behalf of ATU

_____

Signed on behalf of third party

_____

being a duly authorised officer

_____

being a duly authorised officer

_____

Name in block letters

Name in block letters

Description of IT access required by the third party:

Please ensure that both parties retain a signed copy of Appendix A, and forward an additional copy to Cybersecurity@atu.ie