Ollscoil
Teicneolaíochta
an Atlantaigh

Atlantic
Technological
University

User Account Management Policy
Version 1.0

Revision History:

Date of this revision:	24 June 2024
Date of next review:	01 June 2024
Version Number/ Revision Number	1.0
Revision Date	11 October 2024
Summary of Changes	New Policy
Changes Marked	N/A

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 December 2023
Names of Parties in Consultation	UPT
Summary of Changes	Reviewed and approved new policy

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

Approval:

This document requires the following approvals:

Version:	1.0
Approved By:	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:	24 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	Yes

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 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 5
2. Purpose of Policy 5
3. Definitions 5
4. Scope 6
5. Roles and Responsibilities 6
6. Policy Statement 7
   - 6.1 User Accounts 7
   - 6.1 System Owner Managed Accounts 10
7. Exceptions 10
8. Supporting Documents 10

1. Overview/ Introduction

All ATU staff members, students, contractors, and third parties must abide by the relevant ATU information security and access control policies and procedures. ATU will provide all employees, students, contractors and third parties with an ATU IT user account as required to carry out their responsibilities in as effective and efficient manner as possible.

Account Management: User account management procedures must be implemented for user registration, modification and de-registration on all University information systems. These procedures must include a process of monitoring redundant and inactive accounts.

Administrative account: All system created accounts or accounts with administrative privileges shall adhere to the Tiered Administration Model.

2. Purpose of Policy

The purpose of this User Account Management Policy is to detail the method by which ATU IT user identities are managed. The management of ATU IT user accounts is required to ensure security and compliance.

3. Definitions

ATU IT User account: A credential set comprising of a username and password is used to access ATU digital resources. These are uniquely associated with a specific person. These accounts exist in a central repository (i.e., Active Directory, Azure AD) to which systems may federate to access the identity and authentication information.

Administrative Accounts: An account that has more privileges than ordinary users and used to administer a service or system.

Authentication: The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources.

Identity Management System: The creation and maintenance of the unique ATU user accounts across the various systems and applications.

Tiered Administration model: The concept of separating administrative activities from that of a user's standard IT account and IT identity. This identity is specifically provided for the administration of the service or system. This separation from standard identity introduces a security buffer making the administrative account less susceptible to compromise.

Staff Leaver: The term refers to an employee whose contract has ended, retired, or resigned from their position within ATU. They are no longer employed by ATU.

4. Scope

This policy applies to all ATU systems, applications, and other authentication systems which require an identity or account, this includes but is not limited to:

- Network system's authentication.
- Application authentication.
- Laptop, tablet, and portable device authentication.
- MIS Applications.

5. Roles and Responsibilities

ATU IT Services Staff

- To ensure User Account Management conforms to this policy.

ATU IT Operations Managers

- To enforce this policy and monitor compliance with the User Account Management Policy.

- To inform the ATU IT Steering Group of suspected non-compliance and/or suspected breaches of this policy.

ATU Application/System Owners

- To enforce this policy on ATU systems and monitor compliance with the User Account Management Policy.
- To inform the local ATU IT Operations Manager of suspected non-compliance and/or suspected breaches of this policy.

6. Policy Statement

6.1 User Accounts

User Account Management procedures must be implemented for user registration, modification, and de-registration on all ATU systems. All user accounts will be required to comply with ATU Password Standard. Below are the various types of user accounts used within ATU:

Students: Student IT accounts are provided based on a valid student record in the Student Record Management System (SRMS). Student IT accounts provide federated access to other services. Students registered on approved research programmes on the SRMS will be provided with an additional email alias: firstname.surname@research.atu.ie

All Student User accounts are provisioned automatically from the Identity Management System.

Student User accounts may be disabled:

- On instruction from the Registrar's Office
- On indication from the SRMS system.

- If suspicious activity is detected against a student user account to protect the user and University.

Student User accounts shall be purged180 days postdate of disabling.

The Student User account Unique Principal Name (UPN) takes the format of: StudentID@atu.ie

Staff Members: Staff members are provided with a staff user account based on a valid staff record in the College HR System. Staff IT accounts provide federated access to other services.

Depending on the role of staff members, some staff may be provisioned additional accounts on other systems which do not support federated access.

All staff federated user accounts are provisioned from the Identity Management provisioning system.

The Staff User account Unique Principal Name (UPN) takes the format of:

firstname.surname@atu.ie

Staff Leaver: The Staff IT account will be disabled across all federated systems within 48 hours of leaver notification from the College HR system. IT accounts shall be purged180 days postdate of disabling.

Staff accounts may be disabled:

- On instruction from the HR Office
- On indication from the HR Management System.
- If suspicious activity is detected against a staff user account to protect the user and University.
-

Associate User: Associate User accounts are provided for a person who is external to the University and requires access to approved University resources, such as:

- Working in a University office or
- Working on a University project
- Retired staff
- External Examiner
- Visiting lecturer
- Visiting students
- From an agency or 3rd party company
- Contractors

Associate Users will be provided with access to any relevant University services on approval.

The Associate User Account Unique Principal Name (UPN) takes the format of:

first.name.surname@associate.atu.ie

ATU staff members may ‘sponsor’ a person who is not a member of the University community to have access to ATU IT services for the purpose of the business needs of the University. This will require approval by their Head of Function/Department.

Associate User accounts will be for a defined period. Associate accounts will be deleted on expiry date and when access to ATU systems is no longer required.

Associate User accounts may be disabled if suspicious activity is detected against their account to protect the user and University.

6.1 System Owner Managed Accounts

When accounts are created on enterprise authentication systems outside the stewardship of the ATU IT Service department, the unit creating the account must define the procedure by which they will be approved and created. The procedure must adhere with all University standards & policies. In instances where this is not possible due to system constraints, the system owner must conduct a risk analysis and have any risks identified and approved by ATU's Audit and Risk Committee.

7. Exceptions

Any exception to this policy must be documented and formally approved by the IT Governance Committee and Audit and Risk Committee. Policy exceptions must describe:

- The nature of the exception.
- An explanation for why the policy exception is required.
- Any risk created by the policy exception.

8. Supporting Documents

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

- ATU Computing Device Policy
- Information Security Policy
- Acceptable Usage Policy
- Third Party Access Policy
- Password Standard
- Mobile Application Standard
- Web Content Filtering Standard