Identity Management Policy

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH

TU DUBLIN

TECHNOLOGICAL UNIVERSITY DUBLIN

Table of Contents

1. Document Control Summary

Area	Document Information
Author	Infrastructure Solutions Senior Manager
Owner	Head of Technology Services
Reference number	TSIDM2023
Version	1.0
Status	Approved
Approved by / ~~to be approved by~~	University Executive Team & Governing Body
Approval date	11th October 2023
Next review date	11th October 2024
Document Classification	TU Dublin Public

2. Introduction / Context

This document sets out the Technological University Dublin (TU Dublin) Policy for the management of user identities within the University.

User Identities are provided for all eligible users in the University, i.e. employees, students and third parties.

It is important that staff and students are aware of the criteria for the creation of user identities in the University and the lifecycle of those accounts.

3. Purpose

The purpose of this policy is to define the criteria for creating, amending, delisting and maintaining user accounts and access to TU Dublin's IT services and resources, ensuring that all access to IT services and resources is appropriately administered and reviewed.

4. Scope

This policy applies to:

- All staff, students, contractors/consultants, agency staff, vendors and other third parties who are authorised to access TU Dublin IT services and resources.
- All systems, applications and devices in all production stages. (i.e. Development, Test and Production)

Physical access to University buildings and rooms is outside the scope of this policy but it is assumed that the identity management system will be used as a data source for an electronic access control system.

5. Roles and Responsibilities

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

TU Dublin University Executive Team (UET):

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

TU Dublin Chief Operations Officer:

- To ensure the policy is reviewed and approved by the University Executive Team.

Technology Services Senior Management:

- To liaise with the Office of the University Secretary and/or The University Compliance Group on information received in relation to potential breaches of the policy.
- To enforce compliance with this policy where technically possible on TU Dublin systems.

Data Stewards:

- Review the Identity Management policy, and where appropriate, liaise with Technology Services to support the implementation of supporting procedures.

TU Dublin Staff / Students / Third Parties:

- To adhere to the practices contained in this document.
- To report suspected breaches of policy to the IT Service Desk.

6. Definitions

User

- Defined as an individual who possesses a recognized TU Dublin identity. A TU Dublin identity refers to the official credentials, affiliations, or recognition associated with Technological University Dublin

Data Steward

- The individual(s) responsible for a particular set of data – usually the most senior member(s) of a department/function accountable for that department/function's data.

Shared Accounts

- Shared accounts are accounts that use a single pair of credentials to authenticate multiple users. i.e. actions carried out by shared accounts are not attributable to an individual person.

Identity Management system

- Defined as the system that accepts authorised data for Staff, Students and Third Parties from the appropriate source systems and using predefined business rules, creates identity accounts and provisions those accounts to access a variety of University systems according to those business rules.

Listing

- The process of creating and configuring identities used to access applications, systems and data as part of lifecycle management.

Delisting

- Delisting is the act of removing user access to applications, systems and data as part of lifecycle management.

Least Privilege

- Users are provided the minimum access privileges required to carry out their role.

Role Based Access Control

- Users are provided access only to the systems that they require to carry out their role.

Segregation of duties

- User access and duties are segregated and restricted to only the tasks that users/ teams are responsible for.

Third Party Access

- Third Party Access can be defined as “The granting of access to TU Dublin IT resources or data to an individual who is not an Employee or Student of TU Dublin.” Examples of third parties include but are not limited to; Vendors, consultants, contractors, and service providers.

Types of accounts

- **User Accounts -** Unique accounts granting access to TU Dublin IT services and resources attributable to a named individual. i.e. student, staff, and affiliate accounts.
- **Service / Application Accounts -** Accounts required by a system or service in order to authenticate with other systems or applications. These accounts are not associated with individuals.
- **Privileged Accounts -** Privileged accounts are user, system or application accounts that have elevated permissions, for example application admin or super user accounts.

- **Test Accounts -** Accounts created for the purpose of testing the rationale or functionality of hardware/ software.

7. Policy Details:

7.1 Policy Overview

The policy defines the criteria for creating, amending, delisting and maintaining user accounts and access to TU Dublin's IT services and resources, ensuring that all access to IT services and resources is appropriately administered and reviewed.

7.2 Policy Details

7.2.1 Identity Allocation

Wherever possible, an individual user will have a single user account for use across all applications.

This will not be the case where-

- A user is accessing applications in more than one capacity (e.g. they are an employee and a student), it may be necessary to create a secondary user account for that individual in addition to their primary user account.
- The application does not support the use of centrally managed user accounts.
- If privileged or administrative access is required, this will operate with a separate user account

7.2.2 Identity Sources

The Student Records Management System is the single authoritative source of student data for the Identity Management system. Changes in student data, registration status and course enrolment data from the Student Records Management System will drive the identity management process for Students.

The HR System is the single authoritative source of employee data for the Identity Management System. Starters, leavers and changes in staff data from the HR System will drive the identity management process for staff. The Identity Management process for staff relies on the HR system providing information on new joiner start dates, leaving dates and moving dates for existing employees.

Third Party identities are created on request and approved by the appropriate authority.

7.2.3 Identity Requirements

User Access Accounts

- Access to TU Dublin IT services and resources is governed by the use of individual user access accounts and passwords.

- Passwords used to access TU Dublin IT services and resources must comply with the TU Dublin Password Policy.
- Wherever possible, users shall authenticate using single sign on.
- Multi Factor authentication must be used where it is available.
- Credentials used to access TU Dublin IT services and resources must never be shared.
- Users must not use TU Dublin usernames and passwords for any unrelated Third-party services (e.g. Instagram)
- Access rights and privileges to TU Dublin IT services and resources shall be granted using the principle of Role Based Access Control, where access is based on the specific requirement to support the user's role/ area of study.
- The criteria for assigning access privileges must be based on the principle of least privilege and segregation of duties.
- All requests for new user accounts must be submitted to Technology Services in a timely fashion.
- Technology Services shall only create new accounts and amend user/ account permissions on receipt of an appropriately approved request.
- The use of Guest, Temp or Shared/Generic accounts is not permitted. All users must have a named account attributable to them.
- All accounts shall be centrally managed by Technology Services, any requests for exceptions to this rule must be supported by a valid business justification and approved by the Head of Technology Services, or their nominee.
- Users must report known or suspected password compromises to Technology Services at the earliest possible opportunity and change their password immediately.

Service / Application Accounts

- Must be formally requested by the system owner, vendor, project team etc and authorised by the Head of Technology Services, or their nominee.
- May only be created if there is valid justification.
- Must have an assigned owner and a description of their purpose on record.
- Must adhere to the principle of least privilege.
- Service account credentials must be unique to each system or service and must adhere to TU Dublin password policy requirements.
- Must be reviewed and deleted when no longer required.

Test Accounts

- Must be formally requested by the system owner, vendor, project team etc.
- Must be approved by the Head of Technology Services, or their nominee.
- May only be created if justified by the relevant business area/ project team.

- Must have an assigned owner and a description of their purpose on record.
- Must not operate in the production environment.
- Must adhere to TU Dublin password policy requirements.
- Must be reviewed and deleted when no longer required.

Privileged Accounts

- Staff performing administrative tasks with elevated privileges must use a separate account for this purpose.
- The username for privileged accounts should clearly identify the assigned user.
- The elevated privileges assigned to these accounts must follow the principle of the least privileges needed to perform the tasks required by the role.
- May only be created if justified by the relevant business area/ project team.
- Must be approved by the Head of Technology Services, or their nominee.
- Must have an assigned owner and a description of their purpose on record.
- Must be reviewed and deleted when no longer required.

7.2.4 Identity Access Amendments

It is recognised that during a period of employment, a member of staff's job or role may change and therefore their access rights must also be changed accordingly.

- All requests for additional access to specific business applications or data must be formally submitted to Technology Services and approved by the relevant application or data steward.
- Where business application access is not managed by Technology Services, the access request or change must be made directly to the relevant business application owner.
- Technology Services staff shall not grant any additional access without formal approval.
- Automated processes are in place to modify user identity access rights based on source system user account status ie. an individual's registration status in the Student Records Management System
- All requests for access amendments to TU Dublin IT services and resources should be submitted in a timely manner.

7.2.5 Identity Access Reviews

Access to TU Dublin information assets and resources shall be periodically reviewed by data stewards to reduce the risks associated with inappropriate user access.

- Standard user accounts with access to TU Dublin information systems shall be reviewed on a bi-annual basis.
- Privileged user accounts with access to TU Dublin information systems shall be reviewed on a quarterly basis.
- Where an access review identifies an anomaly, a formal request must be submitted (by the data steward) to Technology Services for amendment.

7.2.6 Identity Lifecycle - Joiners & Leavers

Joiners
The Identity Management System is dependent on the quality of data from its source systems and the timeliness of data updates ensure that every user has the appropriate access rights at the correct time.

Identities and basic access rights for employees and students will be created when the data is available in the source system and that individual being in a status eligible for an identity to be created.

If information is provided in a timely manner, staff accounts may be created up to two weeks prior to the start date of the employee.

Leavers
The de-listing of employee and student identities and associated access to IT Services is an automated process based on the status of the account in the Source Identity System.

Employee Identities will be disabled based on the status in the HR System.

Student Identities will be disabled based on their status in the Student Records Management System.

Affiliate, Contractor, Guest and Vendor identities are set to expire either on the date provided by the approver to a maximum of 1 year after creation.

Retired Staff
Staff who are retiring and will continue to be actively involved in the University can apply to retain IT Services as part of the overall Retirement process. These users will be considered as “Active Retired Staff”

“IT Services” are considered Cloud Based Email services and a subset of Library services. Other IT services may be provided on receipt of an approved request.

Access to IT services will be reviewed on an annual basis. Access will be removed automatically if no use of services has taken place over the previous 12 months.

Career Break
Staff who are on a Career Break will retain their access to University email services. Full IT Services access will be restored when they return from their Career Break.

7.3 Approval process

This policy must be approved by both the University Executive Team and Governing Body in order to be considered active.

7.4 Change process

This policy will be reviewed annually or after any significant change to the TU Dublin Identity Systems.

8. Related Documents

This policy should be read in conjunction with the following University policies and Users should ensure compliance with these policies in addition to this policy.

- TU Dublin Information Security Policy
- TU Dublin Password Policy
- TU Dublin Acceptable Use Policy
- TU Dublin Data Protection Policy

9. Appendix

9.1 Queries on this policy

Technology Services

Email: itfeedback@tudublin.ie

10. Document Management

10.1 Version Control

VERSION NUMBER	VERSION DESCRIPTIN / CHANGES MADE	AUTHOR	DATE
Draft 0.6	*Draft created by Technology Services with input from Human Resources and Student Services.*	*Infrastructure Solutions Senior Manager*	*2nd June 2023*
Draft 0.7	*Draft approved by UET, with additional definitions added.*	*Infrastructure Solutions Senior Manager*	*14th June 2023*
Draft 0.8	*Draft approved by ARC, no amendments.*	*Infrastructure Solutions Senior Manager*	*19th September 2023*
Ver 1.0	*Final version approved by GB no amendments.*	*Infrastructure Solutions Senior Manager*	*10th October 2023*

10.2 Document Approval

VERSION NUMBER	APPROVAL DATE	APPROVED BY (NAME AND ROLE)
Draft 0.7	*14th June 2023*	*University Executive Team*
Draft 0.8	*19th September 2023*	*Audit & Risk Committee*
Ver 1.0	*10th October 2023*	*Governing Body*

10.3 Document Ownership

This document is owned by the Head of Technology Services, on behalf of the University.

10.4 Document Review

This document must be reviewed at least every year by Technology Services.

10.5 Document Storage

This document will be stored on the TU Dublin public website.

10.6 Document Classification

This document is classified as TU Dublin Public and is available to all.