MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Data Access Management and Privileged User Policy

28th June 2021

Version: 1.0

www.mtu.ie/policies

Table of Contents

1. Overview ... 3

2. Purpose ... 3

3. Scope ... 4

4. Definitions ... 4

5. Roles and Responsibilities ... 7

6. Policy ... 8

6.1 Policy Requirements for Data Access Management ... 8

6.2 Policy Evidence for Data Access Management ... 9

6.3 Policy Requirements for Data Access Controls ... 9

6.4 Policy Evidence for Data Access Controls ... 9

6.5 Privileged User Policy ... 9

7. Policy Compliance ... 10

7.1 Compliance ... 10

7.2 Compliance Exceptions ... 10

7.3 Non-Compliance ... 10

Document Control ... 12

1. Overview

The University is responsible for the processing of a significant volume of information. These records are evidence of functions and activities performed across the University.

Good quality records are of value to any organisation, and their effective management is necessary to ensure that the records retained. It is vital that everyone is aware of their responsibilities in relation to data protection as follows:

a) comply with information management policies, legal and regulatory requirements (including the Freedom of Information Act 2014, the General Data Protection Regulation 2018), international standards, and best practices;
b) are authentic, reliable and complete;
c) are protected and preserved as evidence to support future actions;
d) ensure current and future accountability;
e) the University has an appointed Data Protection Officer ('DPO') who is available to provide guidance and advice pertaining to this requirement; and,
f) all staff must appropriately protect and handle information in accordance with University policies.

This document aims to inform the efficient management of records to a standard which meets accepted best practice. This Policy shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable law and other binding agreements.

2. Purpose

The purposes of this policy are:

- To ensure there is a process in place to actively manage the life cycle of system and application accounts – their creation, use, dormancy, and deletion -- in order to minimize opportunities for attackers to leverage them;
- To ensure there is a process and tools in place to track/control/prevent/correct/ secure access to critical assets (e.g., information, resources, and systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification; and,
- To ensure that processes and tools are in place and used to track, control, prevent, correct the use of, assignment, and configuration of administrative privileges on computers, networks, and applications.

3. Scope

This policy applies to:

- Any person who is employed by the University who receives, handles or processes data in the course of their employment;
- Any student of the University who receives, handles, or processes data in the course of their studies for administrative, research or any other purpose;
- Third party companies (data processors) that receive, handle, or process data on behalf of the University; and,
- Any person or entities that use University IT resources, during and outside of working hours.

4. Definitions

Administrative Privileges	Having administrator privileges (sometimes called admin rights) means specific staff are granted privileges to perform most, if not all, functions within a system, computer, operating system, or database. For example, these privileges can include such tasks as installing software and hardware drivers, changing system settings, installing system updates. They can also create user accounts and change their passwords.
Content	Content is information with relevant metadata that has a specific use or is used for a particular business purpose.
Data	As used in this Policy shall mean information which either: a) is Processed by means of equipment operating automatically in response to instructions given for that purpose; b) is recorded with the intention that it should be Processed by means of such equipment; c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; d) Does not fall within any of the above, but forms part of a readily accessible record. Data therefore includes any digital data transferred by computer or automated equipment, and any manual information which is part of a relevant filing system.
Data Controller	Means a person or organisation who (alone or with others) determines the purposes for which and the manner in which any personal data are, or are to be, processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.
Data Processor	Means a person or organisation that holds or processes personal data on the instructions of the Data Controller, but does not exercise responsibility for,

	or control over the personal data. An employee of a Data Controller, or a School or Function within a University which is processing personal data for the University as a whole, is not a Data Processor. However, someone who is contracted by the Data Controller to provide a service that involves the processing of personal data would be a Data Processor. It is possible for one University or person to be both a Data Controller and a Data Processor, in respect of distinct sets of personal data. It should be noted however that, if you are uncertain as to whether the University is acting as a Data Processor or a Data Controller of personal data, it should be treated as being the Data Controller (and therefore comply with this policy in full) until confirmation to the contrary is provided by the DPO or Legal team.
Data Subject	Refers to the individual to whom personal data held relates, including employees, students, customers, suppliers.
Metadata	Metadata is a set of data that describes and gives information about other data. It is a description and context of the data. It helps to organize, find and understand data. Examples of metadata include: a) Title and description; b) Tags and categories; c) Who created and when; d) Who last modified and when; e) Who can access or update.
Personal Data	Information which relates to a living individual who is identifiable either directly from the data itself or from the data in conjunction with other information held by the University. Examples of personal data include, but are not limited to: a) Name, email, address, home phone number; b) The contents of an individual student file or HR file; c) A staff appraisal assessment; d) Details about lecture attendance or course work marks; e) Notes of personal supervision, including matters of behaviour and discipline.
Processing	Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The terms ‘Process’ and ‘Processed’ should be construed accordingly.

Privileged User	A privileged user is a user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users.
Records	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.
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.
Systems and Hosts	Means all in-scope hosts (including cloud service, servers, desktop, laptop, network switch, network router/gateway, printer, backup device, etc.)
Third Party	Means an entity, whether or not affiliated with the University, that is in a business arrangement with the University by contract, or otherwise, that warrants ongoing risk management. These Third-Party relationships include, but are not limited to, activities that involve outsourced products and services, use of independent consultants, networking and marketing arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures and other business arrangements where the University has an ongoing relationship. Third Party relationships, for the purposes of this Policy, generally do not include student or customer relationships. Under GDPR a 'Third-Party' means a natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who, under the direct authority of the Data Controller of Data Processor, are authorised to process personal data.

All other terms used in this Policy and any documents issued in support of this Policy, not referenced in this section, shall have the same meaning as the GDPR and/or local requirements.

5. Roles and Responsibilities

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

Responsible Office/Person(s)	Role
Governing Body	• To review and approve the policy on a periodic basis.
President	• Ensure processes and procedures are in place within the University to facilitate adherence to the Data Access Management & Privileged Policy.
University Executive Team	• Implement the Data Access Management & Privileged User policy and advocate a GDPR compliant culture.
Data Protection Officer (DPO)	• To lead the data protection compliance and risk management function, with responsibility for advising how to comply with applicable privacy legislation and regulations, including the GDPR. • To advise on all aspects of data protection and privacy obligations. • To monitor and review all aspects of compliance with data protection and privacy obligations. • To act as a representative of data subjects in relation to the processing of their personal data. • To report directly on data protection risk and compliance to the University Executive Team and the Audit and Risk Committee. • To report directly on data protection risk and compliance to executive management.
IT Manager	• To monitor, where possible in respect of systems and hosts, compliance with the access management requirements in conjunction with system owners, as outlined in Section 6 of this policy. • To inform the Head of Function and Data Protection Officer of suspected non-compliance and/or suspected breaches of the access management requirements (outlined in Section 7).
Head of Department/Function	• To inform the IT department of any staff movement which impacts user access.
Staff/Students/External Parties	• Read and understand this policy document. • Manage information in compliance with this policy. • Contact their Head of School / Function or Data Protection Officer if in any doubt. • To adhere to policy statements in this document.

If you have any queries on the contents of this Policy, please contact a member of the University Executive Team or Data Protection Officer.

6. Policy

This policy should not be viewed in isolation. Rather, it should be considered as part of the University suite of Data Protection and IT policies and procedures.

6.1 Policy Requirements for Data Access Management

a) Establish and enforce a process to ensure that access to system and hosts by all types of end-user (including Administrator end-users) accounts is restricted to ensure that only specific privileges are assigned to end-users commensurate with their role and justification.

b) Configure access for all end-user accounts to systems and hosts through a centralised point of authentication, for example Active Directory or LDAP.

c) Configure network and security devices for centralised authentication, for example TACACS or Radius or similar.

d) Ensure that all access privileges held by all end-user accounts required for the persons role has a valid business justification approved by the data owner.

e) Establish a process to ensure that all privileges held by all end-user accounts are reviewed on a regular basis and any unauthorised access or access held without a valid business justification is remediated immediately. Access must be reviewed immediately in response to new and evolving threats, capabilities, vulnerabilities, customer requirements or experience of security incidents.

f) Establish a process to ensure that all end-user accounts, two-factor authentication tokens held by end of contract/retiring staff are suspended and deleted and all access to end-user accounts held by end of contract/retiring staff is removed in the next provisioning/deprovisioning accounts process. Any re-joining staff must reapply for all access and privileges to systems and hosts.

g) Establish a process to ensure that access for all end-users whose role has changed is modified commensurate with their new role/duties.

h) Ensure that all resources use personally identifiable accounts when accessing any system or host.

6.2 Policy Evidence for Data Access Management

Expected evidence to confirm the operation of this policy:

a) Inventory of end-user accounts including active and disabled accounts (along with date end-user account was deactivated);

b) Assurance report to confirm that end-users accounts in use remain valid and that the privileges held by end-user accounts are authorised with a current legitimate business justification;

c) Assurance report detailing actions taken and the progress against these actions to resolve access that no longer has a valid business justification for all end-user accounts.

6.3 Policy Requirements for Data Access Controls

a) Ensure that all information stored on systems and hosts is protected with file system, network share, application, or database specific access control lists and no sensitive personal data is available to read-only authenticated end-users or world readable.

b) Ensure that archived data (which is not backup data) that is no longer required is removed from systems and hosts or ensure these systems and hosts are removed from the network when there is no longer a valid business justification to retain it. This includes, copies of business data, logs data, configurations, software, system and host device images.

6.4 Policy Evidence for Data Access Controls

Expected evidence to confirm the operation of this policy:

a) Inventory of information repositories (including archive repositories) identifying sensitive information, and the access controls applied to these repositories.

b) Assurance report to confirm that the access controls listed in 6.4(a) are in place and operating as expected.

6.5 Privileged User Policy

The below requirements must be adhered to in order to ensure that the access of all privileged users is managed correctly:

a) Ensure that end-user account with administrative privileges and administrative accounts are only used when explicitly required;

b) Ensure that when Administrators have access to end-user accounts with administrative privileges or administrative accounts there is a documented and legitimate business justification;

c) Ensure that an inventory of all administrative accounts and all accounts with administrative privileges is maintained and validated at regular intervals to ensure that each person with access to administrative privileges is authorised with a current and legitimate business justification. Evidence of each user validation review and justification for access must be maintained;

d) Ensure that administrators are required to access all system and hosts using a fully logged and non-administrative end-user account and transition to an administrative privilege account when required to carry our administrative tasks or duties requiring elevated access;

e) Ensure that third party administrators are required to use a dedicated and hardened VPN/connection gateway server and/or dedicated machine for all administrative connections to the in-scope systems, hosts and network devices in order to perform administrative tasks or tasks requiring elevated access;

f) Ensure sensitive privileged user activity is subject to audit logging and monitoring.

7. Policy Compliance

7.1 Compliance

Breaches of this policy may result in data breaches under data protection legislation, reputational damage to the University and an infringement of the rights of employees or other relevant third parties.

7.2 Compliance Exceptions

Any exception to the policy shall be reported to the Data Protection Officer in advance.

7.3 Non-Compliance

Failure to comply with this policy may lead to disciplinary action, being taken in accordance with the University's disciplinary procedures. Failure of a third-party contractor (or subcontractors) to comply with this policy may lead to termination of the contract and/or legal action.

Non-compliance shall be reported to the Data Protection Officer and/or IT Managers.

Appendix A - Areas Identified for Delayed Compliance

This policy applies to all University accounts and a review must be undertaken on all existing non personal/service/administrative accounts in Cork and Kerry to ensure alignment with the policy.

This review will not be completed by the date of policy approval and some of the accounts within these categories will not be in compliance with the policy for a period of time.

It has been agreed that a full review and alignment can take place post policy approval and will be completed by the deadline outlined below.

Area	Action Required	Timeline
• Service Accounts • Administrative Accounts	• Review all existing accounts;. • Amend and test access rights;	Quarter 3 2023

Document Control

A. Document Details

Title:	Data Access Management and Privileged User Policy
Owner(s):	Vice Presidents for Finance & Administration/Corporate Affairs
Author(s):	Data Protection Officers
This Version Number:	1.0
Status:	Approved
Effective Date:	28/06/2021
Review Date:	06/2022

Important Note: If the 'Status' of this document reads 'Draft', it has not been finalised and should not be relied upon. An existing approved policy is deemed relevant until such time as an updated policy has been approved by the relevant approval authority and becomes the new binding policy.

B. Revision History

Version Number	Revision Date	Summary of Changes	Changes tracked?	Proposed Revision Date
0.1	30/10/2020	Initial Draft of Policy	Yes	
0.2	09/02/2021	Updated based on feedback from DPO's – Overview section, Roles & Responsibilities of DPOs.	Yes	
0.3	02/06/2021	Updated Definitions, Roles and Responsibilities and section 6 based on feedback from IT department and consultation with DPOs on feedback. Added Appendix A.	Yes	

C. Relevant/Related Existing Internal/External Documents

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

D. Consultation History

This document has been prepared in consultation with the following bodies:

E. Approvals

This document requires following approvals (in order where applicable):

Name	Date	Details of Approval Required
Governing Body	28/06/2021	

F. Responsible for Communication and Implementation

The Manager/Functional Area responsible for communication and implementation of the policy:

Title	Functional Area	Date Implemented
Data Protection Officers	Corporate Affairs	28/06/2021