TUS
Ollscoil Teicneolaíochta na Sionainne:
Lár Tíre, An tIarthar Láir
Technological University of the Shannon:
Midlands Midwest

Information Security Policy

COMPUTER SERVICES

Revision History:

Date of this revision: March 2024	**Date of next review:** March 2027

Version Number/ Revision Number	**Revision Date**	**Summary of Changes**	**Changes marked**

Consultation History: See Appendix B

Development and Approval Log:

Responsible for:	**Title**
Policy Developer:	ICT Systems Integration Manager
Policy Owner:	VP Campus Services and Capital Development
Recommended by:	TUS Audit and Risk Committee
Approving Authority:	TUS Governing Body
Reference Documents:	

Approval:

Version	**Approved By:**	**Date**
1.0	TUS Governing Body	25.03.2024

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

Date Approved: **25.03.2024**	**Date Policy to take effect:** **25.03.2024**	**Date Policy to be reviewed:** **25.03.2027**

Document Location:

Website – Policies and Procedures	X
Website – Staff Hub	
Website – Student Hub	
Other – Internal Use Only	Computer Services Policies and Procedures: Technological University of the Shannon: Midwest (tus.ie)

Contents

1. Policy Introduction

This Policy describes how the three key principles of information security, namely confidentiality, integrity of data, and availability of information, are managed by Technological University of the Shannon (TUS). Information Technology (IT, also referred to as ICT) systems used by TUS are critical to all services and activities within TUS. The security of these systems and the data they store and transmit is crucial to ensuring that the business of TUS can operate successfully. The principles are defined and expanded upon under the sub-headings of authorisation, administration, authentication, availability, and auditability, along with additional security considerations and requirements.

2. Purpose of Policy

The purpose of this policy is to define information security management within TUS. The policy sets out how TUS will provide IT resources to users to assist them in performing their duties.

TUS IT Resources will be used only for activities directly associated with the work of TUS. Users are expected to ensure that use of TUS IT Resources is carried out in an acceptable, safe, respectful, and legally compliant manner.

By using any TUS IT Resources, users agree to comply with the terms of this policy. Nothing in this policy affects a person's rights under law.

This policy should be read in conjunction with the Supporting Documentation as outlined in Appendix A.

The policy sets out the overall approach to information security and provides a security model aimed at:

- Protecting TUS Data from unauthorised use, disclosure, modification, damage, or loss.
- Protecting the TUS reputation as well as the work and study environment for staff and students.
- Implementing industry best practice such as recommended by NIST, ISO27001, and vendor best practices, to protect information assets from unauthorised use, disclosure, modification, damage, or loss.
- Providing the required controls by protecting the confidentiality of data, where sensitivity warrants this.
- Preserving the integrity of data, to ensure its completeness and accuracy regardless of confidentiality and criticality.

3. Definitions

Access: access to or using TUS IT Resources from within TUS, and remote access to TUS IT Resources when not onsite at a TUS campus.

AI: refers to all Artificial Intelligence systems, including but not limited to Artificial General Intelligence (AGI) tools, Large Language Model (LLM) based tools, and any other AI systems as may be in general use.

Availability of Information: Availability ensures that IT resources and information are readily available to those who have an authorised requirement to use them.

Confidentiality: Confidentiality restricts information access to authorised users. Confidential data remains confidential and access to data is on a business need-only basis.

CSD: the Computer Services Department, which is the department within TUS that manages access to and administration of IT resources.

Data Protection Legislation: refers to the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), and the Data Protection Acts 1988 – 2018.

Information: in the context of TUS, Information is also referred to as TUS Data.

Information Security: The protection of information systems against unauthorised access to, or modification of, information, whether in storage, processing, or transit, and against the denial of service to authorised users, including those measures necessary to detect, document, and counter such threats. It strives to preserve the confidentiality, integrity, and availability of data and information.

Integrity of data: Integrity protects the accuracy and completeness of information through the controlling of information modifications. Data is and remains accurate and reliable.

Staff: refers to all full-time, part-time and agency employees of TUS.

TUS Data: (including “TUS Master data” and “TUS Transaction data” referred to in this policy) refers to any physical or electronic information stored, processed, or transmitted using TUS IT resources. “TUS Data” is the sole property of TUS, precluding any infringement of Data Protection legislation.

TUS IT Resources: includes but is not limited to:

- End user devices such as desktop PCs, tablets, laptops, and other devices.
- Printers.
- Servers.
- Software systems and applications.
- Network media such as switches and wireless routers.
- Network connectivity (TUS Network).
- TUS supplied Smart Phones and other portable devices.
- All other media and peripheral devices provided by TUS.
- Cloud applications and services provided by TUS.
- Academic scholarly subscription resources provided by TUS.

User: refers to any staff, student, internal (e.g. campus company) or external party who is authorised to use TUS IT Resources and access TUS Data, and who has been given a certain level of access rights (user ID, password, and authorisation levels) to do so.

External Parties: any users who are not employees or students of TUS who have a requirement for access to TUS IT Resources and have been granted this access to perform duties for or on behalf of TUS.

Data Owner: the stakeholder who is responsible for the categorisation, protection, usage, and quality of a TUS data resource.

4. Scope

This policy covers the security of:

- TUS data.
- TUS IT resources.
- TUS devices.
- All other TUS information assets.
- Information Systems including but not limited to all infrastructure, networks, hardware, and software, which are used to manipulate, process, transport or store information owned by TUS.

It applies to usage of all computing and networking facilities and devices provided by any department or functional area of TUS. It should be interpreted so that it has the widest application.

The TUS Information Security Policy and supporting policies apply to all staff and students of TUS and all other users authorised by TUS.

Policy development, review and approval in TUS is co-ordinated through the TUS Corporate Policy Unit, working with the relevant policy stakeholders and policy developers across TUS.

The TUS Information Security Policy should be read in conjunction with the supporting documentation as outlined in Appendix A

5. Roles and Responsibilities

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

5.1 Governing Body:

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

5.2 Vice President for Campus Services and Capital Development:

- To ensure the Policy is reviewed and approved by the Governing Body.
- To consult as appropriate with other Vice Presidents/Deans and their Management Teams.

- To liaise with Vice Presidents/Registrar's Office, Human Resources (HR), or Data Protection officer (DPO) on information received in relation to potential breaches of the policy. Policy breaches that result in TUS data being lost/compromised must be alerted to the DPO.
- To ensure the appropriate standards and procedures are in place to support the policy.

5.3 IT Manager:

- To define and implement best practice, standards and procedures which apply to the policy.
- To oversee, in conjunction with data owners, compliance with the policy and supporting standards and procedures.

5.4 Policy Unit:

- To co-ordinate the development, review, and approval of this policy, in conjunction with relevant stakeholders and policy developer(s).

5.5 All Users:

- To adhere to policy statements in this document.
- To report suspected breaches of policy to their Line Manager/Head of Department and to the IT Servicedesk. Where a violation is of sufficient seriousness, it should also be reported directly to the IT Manager & DPO. Sufficient seriousness in this case refers to policy breaches that constitute compromise or loss of sensitive data, abuse of user privilege, attempted or unauthorised use of another's credentials, or any incident that the Line Manager/Head of Department deems serious enough to alert the IT managers.

5.6 Policy Review Committee

- To review the policy to ensure it meets the requirements of TUS.
- To recommend the policy for the next stage in the Policy Approval process.

6. Policy Statement

In relation to the proper usage of TUS IT Resources, users are required to abide by the law of the State, by this policy, by the Data Protection Legislation and by any additional policies as may be laid down from time to time.

The aim of the Information Security Policy is to ensure the three key principles of information security are implemented in TUS, which include:

- Confidentiality
- Integrity of data
- Availability of information

In terms of these three principles, the policy is set out under the following subheadings which form the building blocks for good practice Information Security:

- *Authorisation*
- *Administration*

- *Authentication*
- *Availability*
- *Auditability*

TUS IT Resources should be used only for activities directly associated with the business of TUS.

6.1 Authorisation

The data owner requests or grants access to the data on behalf of the user; access to IT applications, data, and other relevant resources within TUS is on a business need-only basis. This means, users must be given the minimum level of access considered necessary for the performance of their task or role.

Users who have been granted access to TUS data and IT resources, must take responsibility for ensuring that they comply with relevant data protection legislation and TUS policies and procedures, including but not necessarily limited to those outlined in Appendix A, in relation to the handling and storage of personal data.

To support ongoing operations, authorised CSD administrators do have a legitimate requirement for full access to many key systems and data. The principles of this policy apply to these administrators as well as end users, however it must be clear who has this elevated level of access, who approved this level of access and the reasons why this access is required, as per the CSD Privileged User Access Standard, part of the TUS ICT Standards suite which can be accessed at the IT Servicedesk: TUS ICT Standards : Technological University of the Shannon: Midwest.

On termination of a staff members contract with TUS, all user access to TUS IT resources will be revoked on their date of departure. On approval from the employee's line manager/HoD, a user can be granted access to their account for a period of time post departure to carry out any outstanding duties.

6.2 Administration

Access to TUS data and key IT systems is approved by the relevant data owner. Procedures specific to individual systems guide the administration processes for that system and include indication of the data owner who needs to provide relevant approvals.

Administration processes include:

- User account creation.
- User account amendment.
- User account removal/Deletion.
- Periodic User Account Review.

Note that it is TUS policy to include a review of the system user listings focusing on the validity and appropriateness of access levels in accordance with the relevant internal control guidelines.

6.3 Authentication

TUS systems require usernames/user IDs to identify staff and students, and passwords and/or TUS ID cards to authenticate them. As this is the main authentication mechanism for access to TUS platforms and systems, the TUS Password Standard needs to be strictly applied and adhered to. TUS Password Standard is accessible internally to TUS Staff. Link is provided in the Document Location section of this policy.

In addition to passwords, TUS ID cards are another form of authentication and as such it is prohibited to share TUS ID cards with others.

6.4 Availability

To ensure that TUS data and TUS IT resources are available when required, there are three main layers of controls:

- Prevention of data loss through regular data back-up.
- 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.

6.5 Auditability

An appropriate audit trail of the creation, amendment and deletion of TUS data should be maintained by the information/data owners. This is particularly important in relation to the following:

- TUS Master data including details on staff, students, and suppliers.
- TUS Transaction data including inward fee payments, outward supplier payments, and payroll transactions.
- TUS resource usage data.

Personal data should not be stored on a TUS device as this data is then subject to disclosure under freedom of information requests.

6.6 Other Security Principles

6.6.1 AI Tools

Users of AI tools such as ChatGPT, Google Bard, Midjourney or any other generative AI or LLM system must not enter confidential or sensitive TUS data into the AI system for any purposes. Generative AI/LLM systems store all data entered for their own machine learning to process and can regenerate this information as another answer to any other user of their system. This poses a risk to TUS Information Security which users must be cognisant of when using these systems. Users of AI tools should ensure to be aware of and adhere to any legislation around the use of such tools.

6.6.2 Data Disposal

In accordance with General Data Protection Regulation, all hardware used for the storage of TUS data are to be purged and securely destroyed once it is no longer to be used. When backup media, and other storage devices (including cloud storage) reach

the end of their useful life they are securely purged of TUS data and securely destroyed by CSD or the relevant system or data owner. See TUS Data Retention and Records Management Policy.

6.6.3 Data Storage and Back-up

Staff using workstations/laptops must, where possible, avoid storing TUS data locally on their device. TUS data should be stored on and accessed from the TUS Teams sites, or via the user's TUS OneDrive.

If data is stored locally on a user's workstation, laptop or other device, the user has a responsibility to ensure that all TUS data is backed up. Back-up should be done using at least one of the following methods:

- Regular saving or copying of TUS data to a secure network location such as a personal TUS OneDrive.
- Regularly uploading and saving data to a TUS Teams document library.

All servers holding TUS data are managed and controlled by CSD.

6.6.4 Data Storage and Use

All TUS data is to be stored securely. All confidential data is to be stored on TUS servers or approved cloud services, and not on personal devices, personal cloud storage services and other media. Where there is a specific and authorised requirement to store data on personal devices and other media, these devices should use strong encryption techniques to protect the data.

Staff who access and / or retain any TUS data are responsible for its use and security. Failure to implement adequate measures to protect the confidentiality of TUS data could lead to disciplinary action in accordance with TUS disciplinary procedures.

6.6.5 Data Transmission

All TUS data is to be treated as confidential unless otherwise indicated. It should not be transmitted without adequate precautions being taken to ensure that only the intended recipient can access the data. Appropriate encryption methods as laid out in the TUS Encryption Standard should be used where applicable.

6.6.6 Endpoint protection

All devices that connect to the TUS network must use endpoint protection (anti-virus). All TUS IT resources must run the approved TUS endpoint protection solution. TUS uses industry leading endpoint protection to provide a comprehensive security solution with detection, monitoring, and response capabilities for all TUS endpoints.

TUS reserves the right to disconnect any machine, device or resource that is not deemed to have adequate levels of endpoint protection.

TUS uses whole disk encryption where applicable for all TUS managed mobile devices.

6.6.7 Information Classification and Ownership

All information and Information systems held by TUS must be classified according to TUS's Information Classification Standards. In broad terms, below is a table listing suggested data classification categories:

Not Classified/Public	Information available to the general public and approved for distribution outside TUS.
Internal use only	Information not approved for general distribution outside TUS and which does not clearly fit into the other classifications.
Confidential	Includes data covered by the Data Protection Legislation under the category of personal data (See Note 1 below). Confidential also includes information considered to be commercially sensitive (See Note 2 below) to TUS, including strategic plans and intellectual property.
Strictly Confidential	Includes data covered by the Data Protection Legislation under the category of sensitive personal data or special categories of personal data (See Note 3 below).

Note 1: Personal Data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information. Examples of personal data include a name, address, contact details etc.

Note 2: Commercially Sensitive Data relates to any information held by TUS that if disclosed to an unauthorised party could result in, but is not limited to, the loss of public confidence, non-compliance with regulatory requirements, legal liabilities and additional costs. For example, commercially sensitive information may include, Governing Body reports, senior management board papers, contracts, financial reports, budgets or sensitive project specific information.

Note 3: Sensitive Personal Data (or Special categories of Personal Data) relates to specific categories of personal data which include, amongst other criteria, information relating to the physical and mental health of an individual.

Methods for managing information must be in line with Information Classification Standards, for example, encryption while emailing Confidential Information outside of TUS.

All information and information systems must be assigned an owner. Owners are responsible for controlling access to each of their information assets and information systems to a level of security that matches the value those assets.

6.6.8 Password Standard

All staff including administrators must use strong passwords which match the standards set out in the TUS Password Standard – accessible internally to staff. The link is provided in the document location section of this policy. It is the responsibility of staff to protect their passwords. Passwords should never be written down or shared with others.

If an account or password is suspected to have been compromised, please report the incident to CSD and change all passwords.

6.7 Systems Monitoring

TUS is committed to ensuring robust information security and to protecting users from illegal or damaging actions carried out by groups and/or individuals either knowingly or unknowingly. TUS respects the right to privacy of staff, students, and external parties. However, this right must be balanced against TUS's legitimate right to protect its interests. To achieve its aims in this regard, TUS reserves the right to monitor all TUS IT Resources and TUS Data for operational and security purposes.

When reviewing the results of any monitoring conducted in accordance with this section, TUS will bear in mind that users may be in possession of certain material for legitimate teaching, learning and/or research purposes. Users will not be disadvantaged or subjected to less favourable treatment as a result of TUS monitoring, provided they exercise their academic freedom within the law and can demonstrate that their teachings, research or qualifications are relevant to material detected and results revealed by TUS monitoring.

Monitoring of activity on or using TUS IT Resources does not impact on the confidentiality of research or other data stored for the purposes of research projects. Any queries relating to the confidentiality of data stored on individual systems as related to the monitoring and logging of system data for operational and security purposes should be raised with the IT managers.

Computer Services will carry out cybersecurity awareness and training exercises 3-4 times per semester to simulate phishing and other attack vectors as part of the ongoing training of users in the risks associated with various elements of working and operating online.

6.8 Who to Contact

If you have any queries on this policy and/or if you want to report a suspected security breach, including a password or access break, or a lost/stolen storage device, please contact the IT Servicedesk in the first instance and then the IT Manager as may be required.

In addition, if you have any issues in relation to passwords, data backups, encryption, data protection and any information security or IT acceptable usage issue please contact the IT Servicedesk in the first instance and then the IT Manager as may be required.

7. Policy Compliance / Monitoring and Review

7.1 Policy Acceptance

By using any TUS IT Resources, users agree to comply with the terms of this Policy.

7.2 Violation of Policy

Contravention of any of the above policy can lead to:

- The removal of TUS resource privileges.
- Disciplinary action in accordance with the applicable TUS disciplinary procedure.

Failure of an individual student or member of staff to comply with this policy may lead to the instigation of the relevant disciplinary procedures and, in certain circumstances, legal action may be taken.

Failure of a contractor to comply could lead to the cancellation of a contract.

7.3 Monitoring and Review

This policy will be monitored and reviewed periodically, and at least every three years, to ensure that it is in line with the TUS Internal Control Framework and with overall TUS policy and procedures, and that it accurately reflects the legislative and other requirements of TUS in this area.

Appendix A - Supporting Documentation

- TUS Acceptable Usage Policy.
- TUS ICT Standards document.

The above list is not exhaustive and other TUS documents may also be relevant.
TUS acceptable usage falls under the scope of several pieces of legislation, including but not limited to:

- General Data Protection Regulation.
- Data Protection Acts, 1998 – 2018.
- European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (as amended).
- Criminal Damage Act, 1991(as amended).
- Copyright and Related Rights Acts, 2000 (as amended).
- Electronic Commerce Act 2000 (as amended).
- Prohibition of Incitement to Hatred Act, 1989 (as amended).
- Freedom of Information Act 2014 (as amended).
- Protected Disclosures Act, 2014 (as amended).
- Child Trafficking & Pornography Act, 1998 (as amended).
- Equal Status Act, 2000 (as amended).
- Criminal Justice Act, 2011 (as amended).

Appendix B - Consultation History:

NOTE: TUS Policy Review Committee for the TUS Information Security Policy consisted of:

- Vice President, Campus Services and Capital Development.
- IT Managers, Midlands and Midwest.
- ICT Systems Integration Manager.
- Information and Compliance Officer.
- HR Project Manager.

Version Number/ Revision Number	**Consultation Date**	**Names of Parties in Consultation**	**Summary of Changes**
0.1	01/09/2021	ICT Department	Initial draft
0.2	28/3/22	ICT Department	Data storage – cloud services added
0.3	6/1/23	ICT Department	Changed short form from TUSMM to TUS to reflect common usage
0.4	5/10/23	ICT Department, ICO	Clause added on use of AI Tools, under section 6. Policy Statement, sub-heading Authorisation – Data Transmission
0.5	11/10/2023	ICT Department, ICO	Introduction expanded Added HR to Roles and Responsibilities Added approval required from manager/HoD for TUS mail to be forwarded after employee termination Removed ref to departmental shares (replaced by Teams)

0.6	22/11/23	Policy Review Committee	Reviewed and agreed by PRC
0.7	10/1/24	TUS ARC	Amendments made based on TUS Audit and Risk committee feedback. Policy statement reorganised for readability. Added Policy Unit to Roles and Responsibilities. Expanded terminology for clarity. Added Information Clarification section under Other Considerations.
0.7	9/22024	Privacy Engine - Data Privacy Management Platform & Data Protection Consultancy for GDPR, CCPA, HIPPAA and SOC 2.	Following a review from Privacy Engine there were additions in section 6.6.2 and 6.6.8 which now provide links to related documents.
0.8	27/2/2024	Audit and Risk Committee Review	6.1 (p.8) - Added link to CSD Privileged User Access policy, 6.3 (p.8)– reply to note explaining how password standards are enforced – no change to policy wording

			6.6.3 (p10) – reply to note regarding personal data backup for TUS users – no change to policy wording. 6.7 (p.12) – changed '*from time to time'* to *'3-4 times per semester*'
0.9	6/3/2024	Audit and Risk Committee Review	Section 3 - Definitions re-ordered alphabetically. Definition of Information Security added to list. Section 5.5 - Edited for consistency with AUP. - Guideline sentence added. Section 6.1 – changed 'employee' to 'staff member'. Item 6.7 – removed sentence "direction from a member of TUS Management through the IT Manager" – confusing language. Section 6.7 – changed "CSD Helpdesk" to "IT Servicedesk".

8. Consultation and Communication Plan Detail

Please complete the relevant information below:

IDENTIFIED NEED:

A requirement for TUS to have an Information Security Policy

STAKEHOLDERS:

All TUS employees and students

PROPOSED TIMELINE FOR CONSULTATION:

July 2023 to November 2023

CONSULTATION GROUP COMPOSITION (REVIEW GROUP) (IF NECESSARY)

TUS VP Corporate Services and Capital Development, IT Manager – TUS Midlands, ICT Systems Integration Manager, IT Manager TUS Midwest, TUS HR Project Manager, Head of Design in LSAD, TUS Information and Data Compliance Officer

PROPOSED TIMELINE FROM DRAFT TO IMPLEMENTATION:

August 2023 to January 2024

BEST PRACTICE REFERENCES:

LEGISLATIVE REQUIREMENTS / REFERENCES:

APPROVING COMMITTEE/S:

Audit and Risk Committee – review and recommendation to the Governing Body for approval.
Governing Body – Approval

PUBLICATION AND INFORMATION PLAN:

Website, Staff Portal and Functional Managers

MONITOR AND REVIEW PROPOSAL:

Monitor Annually, review every three years.