TU Technology Acceptable Usage Policy

The Acceptable Usage Policy (AUP) applies to anyone using Tusculum University technology resources.

Last Updated by Information Systems April 2025

This AUP defines responsible and appropriate usage of Tusculum University's Information Technology resources in fulfillment of the Mission of the University. It applies to everyone using the University's Information Technology Resources.

Responsible, appropriate usage is always ethical, reflects honesty in all work, shows stewardship in the consumption of shared resources, and is guided by Christian principles.

This AUP will not be static, due to the dynamic nature of technological advances. The University reserves the right to amend, to modify or to strengthen this AUP at any time and without prior notice, to maintain and to enhance the definition of acceptable usage.

I. Policy Objective

A. **REASON FOR POLICY**
Because Clients may have access to (1) sensitive information due to their University roles and (2) shared resources, it is imperative that behavior and activities always comply with this AUP.

B. **SCOPE OF POLICY AND ENTITIES AFFECTED**
The AUP governs use of all Information Technology Resources and all Client Resources, regardless of location. Each Client always assumes responsibility for his or her own behavior while utilizing any Information Systems Resources. Failure to comply with this AUP may adversely affect the Mission of the University and may result in Client disciplinary action.

Additionally, the University reserves the right to remove or to restrict a Client's privileges and access to Information Systems Resources without notice, as needed to maintain appropriate and secure use of Information Systems Resources.

Any knowledge of a violation of this AUP must be immediately reported to the employee's supervisor and to the Director of Information Systems or his or her designee.

II. Definitions

Throughout this AUP, the following terms will have these specific associated meanings:

- **Client** - current or prospective students, current or prospective employees, alumni, retirees, volunteers or guests of the University who use Information Technology Resources
- **Information Technology Resources** - resources owned, leased, licensed or used by Tusculum University that include but are not limited to software, hardware, wireless and physical networking equipment/services, telecommunication equipment, computer labs, workstations, media equipment, storage devices (CDs, DVDs, USB drives, network drives, removable drives,

solid-state drives), cloud-based services (Microsoft OneDrive, Teams, Zoom, etc.), internet service, email, externally-hosted or on-premise services, academic systems (Instructure Canvas LMS, etc.), Enterprise Information Systems (Ellucian Colleague, SelfService,, Microsoft SharePoint, Teams, Zoom, etc.), data/information, digital assets, etc.

- **Client Resources** - resources owned, leased, licensed or used by Clients to utilize Information Technology Resources in any way that include but are not limited to computers, tablets, smartphones, displays, cloud-based services, gaming consoles, printers, etc.
- **Department of Information Systems** (TDIS)- the group of designated University staff members who maintain Information Technology Resources (TDIS is not responsible for installing, supporting or maintaining Client Resources).

III. Policy Content

A. CLIENT ACCESS AND PRIVILEGES

1. Access Provision

The University provides appropriate access to Information Systems Resources, based on Client roles and requirements. Each student receives initial account access upon acceptance to the University. Each employee receives access on or before his or her official date of employment, as determined by the Office of Human Resources.

2. Client Credentials

Selected Clients (current students and current employees) will each be issued account credentials (a unique account name and a private password) to provide this access. Each of those Clients is responsible for all activities performed using his or her credentials.

Each password is an essential element of the University's information security. A strong University password, different from the Client's non-University passwords, is the front line of protection. Each Client is responsible for maintaining password confidentiality by never sharing a password with another person. Each Client should change his or her password periodically to help ensure a high level of University security.

Any suspected unauthorized use of Client credentials must be reported immediately to the IS Help Desk at TDIS@tusculum.edu or 423-636-7346

3. Access Termination

Each enrolled student's account access is disabled 182 days after the last date of the student's active enrollment at the University. For accepted students who did not enroll in classes, account access is disabled two days after the end date of the term for which the student applied. When account access ends, all files, email, and other content associated with the student's technology accounts will be deleted.

Employee access will be terminated upon notification of the employee's separation by the Office of Human Resources. The employee's supervisor or other authorized University administrator may request from the Office of Human Resources that the employee's files, email, and other content be maintained for review or for reassignment to another employee.

Information Systems Resources assigned to the employee (computer, monitors, laptop, printer, etc.) are subject to IS's Equipment Disposition policy.

4. Use of Client Resources on University Networks

Client Resources have access to use the University's wireless networks to the extent that use does not pose security threats, network limitations, or potential/actual disruption of network services.

Employees may connect Client Resources to the secure staff wireless network to access Information Systems Resources provided they adhere to the strict guidelines of data stewardship defined throughout this AUP. Students may connect Client Resources to the student wireless network provided they adhere to acceptable usage guidelines defined throughout this AUP.

Clients are not allowed to use Client Resources on the University's wired staff network for any purpose without prior approval from Information Systems. Students are allowed to use Client Resources on the wired ResNet student network.

Information Systems reserves the right to change or restrict Client Resource access to network access for the protection of Information Systems Resources, without prior notice.

B. ACCEPTABLE, UNACCEPTABLE AND UNAUTHORIZED USAGE

1. Acceptable Usage of Information Systems Resources

As stated in the AUP's Rationale, Clients receive access to Information Systems Resources in fulfillment of the Mission of the University. Usage guided by the Mission and the University's Core Values is considered acceptable.

2. Unacceptable Usage of Information Systems Resources

Unacceptable, prohibited usage of Information Systems Resources includes but is not limited to:

1. transmitting, displaying, printing, or storing any material/software in violation of any federal, state, or local laws including copyright law;
2. transmitting, displaying, printing, or storing inappropriate material, including but not limited to:
    1. text, images, video, audio, or other digital content, with the purpose to harass, intimidate, threaten, abuse, illegally discriminate against, or offend another person on the basis of race, color, religion, sex, national origin, age, disability, or genetic information;

        2. sexually explicit, obscene, or pornographic comments or images;
        3. fraudulent content;
    3. using Information Technology Resources to harass or bother, whether or not an actual message is communicated, or where no purpose for communication exists, or where the recipient has expressed a desire for the communication to cease;
    4. disrupting or damaging administrative, academic, or related activities of another Client;
    5. violating or threatening to violate the privacy of another Client;
    6. forging email or other digital communications;
    7. distributing unsolicited or unwelcome email or other digital communications;
    8. installing or using any unauthorized Peer-to-Peer (P2P) file-sharing service;
    9. connecting Client Resources to Information Systems Resources except as allowed by AUP III.A.4;
    10. engaging in or promoting illegal, unethical, or harmful activities;
    11. engaging in any other practice or activity that, in the opinion of the University administration, constitutes unacceptable behavior, results in the misuse of Information Systems Resources, or jeopardizes the operation of Information Systems Resources.

If, in the interest of authentic academic or administrative work, a Client needs to perform a specific task considered unacceptable, a request to perform the specific task must be submitted in advance by the student and his or her supervising employee, or by the employee and his or her supervisor, for review by the Director of Information Systems.

Commercial and not-for-profit uses of Information Systems Resources are prohibited unless formally authorized by University administration. Clients are expected to be responsible stewards of Information Systems Resources and to limit use to activities related to the Mission of the University.

3. **Usage of Learning Spaces**

Learning spaces include computing labs, discipline-specific labs, classrooms, libraries, various common areas, other venues, etc. and associated Information Systems Resources. Each learning space is available when not in use for a class, scheduled meeting, or other University-approved event. However, use may be subject to approval by the department responsible for the specific learning space.

Clients are expected to use learning spaces in a responsible manner, as defined in this AUP. Clients must not cause disruption, display abusive or inappropriate behavior towards other Clients, or create disturbances.

4. Usage of Workstations

University-owned workstations in learning spaces, offices, and other University locations are configured with University-approved software and are maintained by Information Systems. Clients must not attempt to change the configuration on these workstations unless authorized in advance by Information Systems leadership. Unauthorized changes must be reported immediately to the Information Systems Help Desk TDIS@tusculum.edu or 423-636-7346 (or x5346).

C. PRIVACY AND INFORMATION SYSTEMS RESOURCES

Information security is mandated by the federal government through the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), and other legislation. Lack of compliance can result in substantial institutional fines as well as individual fines or imprisonment. Your part in this compliance is essential to the mission of Tusculum University.

1. Privacy Expectations for Information Technology Resources

The University has no obligation to monitor file/message content residing on or flowing through the University's information systems. However, the University reserves the right to review or remove any message, file, database, media, or other material from its Information Technology Resources to secure and protect the data resources of the University.

At any time, without prior notice and for any reason, the University reserves the right to examine or to monitor:

a. any Information Technology Resources including email, voicemail, network/workstation/portable/hosted files, and directories;

b. any Client Resource using or connected to Information Technology Resources;

c. Internet use of Clients using the University's wired or wireless networks.

These examinations are performed to assure compliance with this AUP, federal and state laws, and other University policies, to support internal investigations, to comply with legal requirements, such as a subpoena or court order, or to assist with the management of Information Systems Resources.

2. Disclaimer of Responsibility for Damage to Data, Software, or Hardware

The University uses access controls and other security measures to protect confidentiality, integrity, and availability of the information associated with Information Systems Resources. In keeping with these objectives, the University maintains the authority (1) to restrict or revoke any Client's access, (2) to inspect, copy, remove, or otherwise alter any Information Systems Resources that may undermine these objectives, and (3) to take any other steps deemed necessary to manage and to protect Information Systems Resources. The University disclaims any responsibility for loss or damage to data, software, or hardware that results from its efforts to meet these security objectives.

3. Treatment of University Confidential and Proprietary Information

University-generated programs, system files, programming codes, and related documentation are confidential and must not be removed, tampered with, altered, or destroyed when an employee, student worker, consultant, or contractor leaves the employ of the University.

4. Treatment of Third-Party Confidential and Proprietary Information

Unless specified otherwise by contract, all confidential or proprietary information, including software, databases, and system resources entrusted to the University by a third party must be protected by University employees as though it were the University's confidential information.

5. Storage of Sensitive Information on Portable, Networked or Remote Resources

Portable, networked, or remote data devices/systems can provide Clients convenient remote access to the University's data for business purposes. These devices/systems are included in the list of Information Systems Resources.

Employees, including student workers, must protect any sensitive and personally identifiable information (PII) stored on portable, networked, or remote data devices/systems from unauthorized access.

This must be done through the use of appropriate measures, including, but not limited to:

- disk and file encryption
- effective password protection
- up-to-date virus protection and malware detection/removal products
- use of data-destruction procedures when information is no longer needed
- use of practices for purging, overwriting, or degaussing equipment when ownership changes
- reasonable safeguards to prevent theft of the device and/or viewing protected information
- use of multi-factor authentication
- use of data loss prevention (DLP) services
- adherence to GLBA, GDPR, HIPPA, FERPA, and other regulatory requirements
- limitation of protected data and PII stored on the device to the "minimum necessary" to accomplish the purpose

. Training in the use of PII by the employee's immediate supervisor or designee, Information Systems, or the Office of Human Resources at the time of hiring.

6. Privacy Expectations for Administrative Data

It is imperative that all administrative data are received, stored, and maintained by University employees (including student workers) in a secure and confidential manner. This information is stored in a variety of formats including printed documents, electronic databases, digital files, and document images.

The University is responsible for the accuracy, integrity, and confidentiality of this data. Data must be treated as confidential unless approved for public release. By law, certain electronic institutional data are confidential and may not be released without proper authorization to the appropriate requester. Professional or personal behavior can affect or threaten the security and confidentiality of University data.

All employees accessing the University's Enterprise Information Systems are required to adhere to the following policies. They are required to sign the Employee Confidentiality Agreement upon employment. That agreement is included as an addendum to the Faculty Handbook, the Staff Handbook, the Student Employment Handbook, and all other relevant area-specific employee documents.

. Unauthorized use of any information in files maintained, stored, or processed by Information Systems Resources is prohibited.

a. No Client is permitted to seek personal benefit or to allow others to benefit personally from the contents of any University data.

b. No Client is permitted to distribute data except as defined by the University.

c. No Client shall knowingly include, or cause to be included, in any record or report, a false, inaccurate, or misleading entry. No one will knowingly change or delete or cause to be changed or deleted an entry in any record or report, unless expressly authorized to do so and in accordance with Tusculum University's Faculty Handbook, Staff Handbook, Student Employment Handbook, or other related policies and procedures.

d. No official record or report, or copy thereof, shall be removed from the office where it is maintained or copied or printed via electronic means except in the authorized performance of a person's duties and in accordance with established procedures of the University. Copies made for the performance of a person's duties shall not be released to third parties except when required by a work assignment.

e. Information Technology Resources, when not in use, must be locked by a standard operating-system, keypad, or other password-locking mechanism.

f. No one is to aid, abet, or conspire with another to violate any part of these policies.

g. Client responsibility for information security, confidentiality, and integrity continues after leaving a position or employment at the University.

h. Clients must report violations to a supervisor or to the Office of Human Resources, as soon as possible.

D. INTELLECTUAL PROPERTY

Respect for the intellectual property of others is essential to the Mission of the University. Unless specific ownership of intellectual property has been established in accordance with the University's

Copyright & Intellectual Property Policies (see Faculty Handbook), the University retains legal ownership of the contents of all Information Systems Resources.

The University's institutional data will not be released to internal or external entities, graduate students, or undergraduate students without expressed, written approval from University Administration.

1. **Copyright Laws**

Clients are expected to follow the University's Copyright & Intellectual Property Policies. Those policies adhere to laws regulating the use, distribution, and reproduction of copyrighted works. They also provide clear guidelines for permissible copying under the fair-use doctrine, while maximizing the educational benefits of using copyrighted materials in the classroom and in other educational settings.

Works protected by copyright may not be accessed or distributed by file sharing, peer-to-peer technology, or any other method violating sections 501-513 of the United States Code Title 17.

2. **Software Licenses**

The University strongly supports strict adherence to license agreements and copyright holder notices. Duplication or distribution of software materials without the permission of the copyright owner is illegal.

Only software that supports the Mission of the University should be used on Information Systems Resources. That software includes but is not limited to:

- software purchased and installed by Information Systems under a site agreement;
- software purchased as a single copy and installed by Information Systems on a single device;
- software developed by employees or students;
- public-domain software and software contributed to the University;
- freely available software that may not be in the public domain, such as software licensed under General Public License (GPL)
- software licensed under software-as-a-service (SaaS/cloud-based) agreement

Illegal copies of copyrighted software may not be made or used on Information Technology Resources. The legal or insurance-indemnification protection of the University and its Trustees will not be extended to employees or students who violate copyright laws. Software not acquired by the University via an officially sanctioned means as stated above will not be installed or operated on Information Technology Resources.

- **Trial Licenses for Software**

Freeware, shareware, and trial-ware are covered by copyright and are subject to the terms and conditions defined by the holder of the copyright and by copyright policies of the University.

- **Fair Use**

Unless permission from the copyright owner(s) is first obtained, making multiple copies of materials from magazines, journals, newsletters, software documentation, and other publications is prohibited unless it is both reasonable and customary. This notice of "fair use" is in keeping with copyright laws as referenced at copyright.gov

- **DISCIPLINARY ACTION**

Disciplinary action shall follow existing University policies and procedures governed by the applicable provisions of the Student Handbook, Faculty Handbook or Staff handbook, and by the applicable local, state, and federal laws.

The following disciplinary sanctions outline some, but not necessarily all, actions that may be taken either singularly or in combination by the University against violators of this AUP:

  - warning to notify the individual that continuation or repetition of specified conduct may be cause for other disciplinary action;
  - reprimand in writing indicating further violation may result in more serious penalties;
  - restriction of Information Systems Resource privileges for a specified period;
  - University probation, suspension, or expulsion;
  - restitution to reimburse the University for damage to or misuse of Information Systems Resources or facilities.

During an investigation, any of these disciplinary sanctions may be applied until a final determination has been made in regard to the charges made against the individual. In the event that other University regulations are violated, additional penalties may be imposed. Information concerning illegal use of Information Systems Resources shall be turned over to law enforcement agencies for possible felony prosecution.

- **POLICY REVIEW PROCESS**
  This policy will be periodically reviewed to make appropriate adjustments to the AUP, to update risk assessment and remediation, and to review and update material. Please submit policy questions, comments, suggtestions, etc. to the Director of Information Systems (Chris Summey csummey@tusculum.edu).