



Faculty, Staff and Student support

Daytime

Help Desk Hours – 8am – 5pm M – F

Location – Niswonger Commons Building 4th Floor

Email – tdis@tusculum.edu – this email address goes to every member of the Information Systems Team. So the member of the IS team that needs to handle the issue gets it and takes care of it.

Help Desk Phone line – 423-636-7346. IF YOU LEAVE A MESSAGE IT GENERATES AN AUTOMATED EMAIL TO THE ENTIRE INFORMATION SYSTEMS TEAM AND THE PROPER TECHNICIAN WILL RESPOND. (Internal extension 5346)

Moodle Password Reset (for students)

<https://elearn.tusculum.edu/moodle/login/index.php> click the lost password link and a new one will be sent to your Tusculum University Student email address. Passwords will not be sent to any other email address other than the Tusculum student assigned one.

PLEASE NOTE: If you email the help desk from an email address other than the Tusculum issued account password information will not be sent. If you cannot get into your Tusculum account to access the email then you will need to call and leave a phone number that you can be reached at.

After Hours

Email – tdis@tusculum.edu – this email address goes to every member of the Information Systems Team. So the member of the IS team that needs to handle the issue gets it and takes care of it.

Help Desk Phone line – 423-636-7346. IF YOU LEAVE A MESSAGE IT GENERATES AN AUTOMATED EMAIL TO THE ENTIRE INFORMATION SYSTEMS TEAM AND THE PROPER TECHNICIAN WILL RESPOND EITHER WHEN THE EMAIL IS RECEIVED OR IF IT IS TOO LATE IN THE NIGHT, FIRST THING IN THE MORNING.

- Remember that if you would like for a technician to call you back, you need to leave a phone number.

Secondary after Hours Phone number

423.470.2942



Infrastructure Information

Bandwidth:

ENA provided ingress/egress is 1Gb. Student LAN gets 100Mbps ingress/egress (200Mbps burstable). Staff LAN is behind Cisco ASA 5510 as is the Barracuda Spam Firewall. Knoxville and Morristown satellite sites are behind the same ASA firewall and connected to the main campus via ENA fiber Ethernet at 100Mbps.

Backups:

The Cisco ASA firewall protects the internal network from the outside world as well as Windows servers and clients running Windows Firewall. Moodle data is backed up daily. Also, all file server data is backed up either nightly or weekly (on servers that data doesn't change as much). All of these backups run automatically also.

Storage:

We currently have over 300 terabytes of storage allocated for Virtual servers

LMS – Our learning management platform (Moodle)

- Currently running version 3.3
- LMS platform I snow in Tusculum's Cloud environment, hosted in Nashville and replicated nightly to data centers in Indianapolis and Atlanta)
- Moodle is now synced with our Active directory so students use the same password for our LMS as they would for any lab.

Video conferencing:

- Currently have 40 ZOOM licenses allowing for synchronous delivery of curriculum.
- Integrated "Big Blue Button" with Moodle so Faculty can conduct synchronous communication with students.

Summary:

Tusculum University has the infrastructure to support a major influx of students for any of our existing programs and is agile enough to add new programs as they are developed and approved.



Information Security Policy

ERP Systems— Tusculum University. Tusculum's ERP system (Colleague) is housed in Charleston WVA by Independent College Enterprise (ICE). A list of the systems covered by the ICE information policies are listed below this policy.

Policy Statement

It is ICE's policy to ensure that information stored and managed by ICE will be protected from a loss of:

- Confidentiality – making information only accessible to authorized individuals
- Integrity – safeguarding the accuracy and completeness of information and processing methods
- Availability – authorized users have access to the information when required.

The document provides a framework for managing information security. It is a high level document and other controls, such as standards, processes, procedure, training and tools, are designed to supplement the policy.

Asset Management

- All assets (data, information, software, computer and communications equipment, service utilities) will be identified and assigned a person responsible for the asset.
- Those identified persons are responsible for the maintenance and protection of the assets.

Human Resource Security

- Security responsibilities will be included in job descriptions and in terms of conditions of employment.
- Verification checks will be carried out on all new employees.
- Agreements with contractors and third parties will include a statement agreeing to adhere to stringent security practices that minimally comply with current laws and regulations.

Physical and Environmental Security

- Critical or sensitive information processing facilities will be housed in secure areas.
- The secure areas will be protected by defined security perimeters with appropriate barriers and entry controls.

- Critical and sensitive information will be physically protected from unauthorized access, damage and interference.

Access Control

- Access to all information will be controlled
- Access to information and information systems will be driven by business requirements. Access will be granted to employees, contractors and other stakeholders according to role and only to a level that allows each to carry out duties
- A formal user registration and deregistration procedure will be implemented for access to all information systems and services.

Information Security Responsibilities

- The Vice President / Chief Technology Officer is the designated owner of the policy is responsible for the maintenance and review of the policy.
- Tusculum network and sys administrators, programmers and analysts are responsible for developing and maintaining procedures that support the policy
- TDIS staff and Cabinet will periodically review and make recommendation on the policy, standards, and procedures
- The Tusculum University Board of Trustees approves policy and updates to the policy
- Anyone who has access to TCDIS systems and information are required to adhere to the Information Security Policy, processes and procedures

Systems Covered

Raiser's Edge:

- IA

Synoptix:

- Accounts Payable/General Ledger

Colleague/Informer/SoftDocs:

- Financial Aid
- Business Office
- Accounts Payable
- Payroll
- Registrar
- Admission


- Student Affairs
- Institutional Research
- Advising
- Athletics
- Academics
- Faculty Services
- Information Technology
- Human Resources

Tusculum On Site Information Security procedures

- **Safeguarding NPI**
Tusculum protects nonpublic personal information (NPI) by
 - limiting user access,
 - masking fields by default within the SIS
 - controlling printed material

- We do not disclose account numbers or financial codes for marketing purposes
- Tusculum uses a student ID number instead of the SSN for identification purposes.
- Student SSN and DOB are masked by default, and only staff who have business need to view have access
- Only financial aid staff, finance office and business office have read/write to the primary FA screens
- Only certain FA staff have access to the FA config and setup screens within Colleague
- Individuals outside of FA who request access to FA are approved by the Director of FA for access and then that access is usually Inquiry level, meaning they can see but not change.
- Reporting and FA reports with Informer and TUreports are controlled, so that only users who have need-to-know may access FA reports
- Students may only view their own awards within WebAdvisor. They are not allowed to change loan/award amounts.
- Printers can be set to hold sensitive documents (such as award info) until a PIN is entered, so that printouts aren't unattended.
- Scanned documents that move to ICE are across an encrypted VPN.
- All faculty/staff and student workers must take FERPA tutorial and submit a form that states they understand the importance of FERPA and not sharing student PII
- Files or documents leaving TU network either are sent within an encrypted, password-protected ZIP file or are sent over an encrypted connection
- All students complete the Student Loan Entrance Counseling and Exit Counseling online at <https://www.studentloans.gov/myDirectLoan/index.action> . Financial Aid receives an import file of who completed the counseling.

Account Password Policies

Policy ▲	Policy Setting
 Enforce password history	2 passwords remembered
 Maximum password age	90 days
 Minimum password age	0 days
 Minimum password length	7 characters
 Password must meet complexity requirements	Enabled
 Store passwords using reversible encryption	Disabled

Account Lockout Policy

Policy ▲	Policy Setting
 Account lockout duration	15 minutes
 Account lockout threshold	5 invalid logon attempts
 Reset account lockout counter after	15 minutes

Student Notifications: Every student is given this notice regarding their account access

Dear:

As a student at Tusculum University, a personalized e-mail account has been created for you.

E-mail ID / Moodle Username:

Lab UserID:

Email/ Moodle / Lab Password:

This e-mail account will be used by all Tusculum University offices (e.g., Academic Advising, Admissions, the Bookstore, the Business Office, the Financial Aid Office, and the Library) and faculty for future correspondence. In addition to school-related business, you may use this e-mail account for your personal correspondence. Please note that there is a storage limit on the account; therefore, in order for the e-mail to properly function it is necessary to delete any obsolete messages in a timely manner.

Your e-mail account can be accessed at <https://www.outlook.com/students.tusculum.edu>. The website will prompt you to enter the username and password indicated above. You will be prompted to change your email password at first login attempt. You will also be asked security information, so if you forget your password, a reset can be sent to an alternative account.

Moodle is our Learning Management System (LMS). Moodle can be accessed at <https://elearn.tusculum.edu/moodle/login/index.php>. The website will prompt you for your userID and password given above. The focus of the Moodle project is always on giving educators the best tools to manage and promote learning.

Should you encounter any problems, or have any questions regarding the use of your Moodle or e-mail account, please contact the Information Systems

Conditions of University Access (Privacy Policy)

In accordance with state and federal law, Tusculum may access all aspects of IT Systems, without the consent of the User, in the following circumstances

- When necessary to identify or diagnose systems or security Vulnerabilities and problems, or otherwise preserve the integrity of the IT Systems
- When required by federal, state, or local law or administrative rules
- When there are reasonable grounds to believe that a violation of law or a significant breach of Tusculum policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct
- When such access to IT Systems is required to carry out essential business functions of the University
- When required to preserve public health and safety

From the Student Handbook / online version of handbook:

- **NOTICE TO USERS:** It is the policy of Tusculum University to protect all institutional computing resources including, but not limited to, hardware and software, consisting of the actual equipment being supplied by the university as well as the programs and related materials used in conjunction therewith. In accordance with local, state, and federal law, indiscriminate examination of individual's files is not permitted, nonetheless as a means of maintaining the integrity and security of those aforementioned resources. Tusculum University retains the right to inspect accounts and files stored on any system owned, maintained and/or leased by said University. While no prior authorization by individual users is required to inspect those files and accounts, you are, by virtue of accepting the account offered by Tusculum University and "logging" on to its computing equipment, granting to the University prior unrestricted permission, subject to University policy, to review, examine and/or otherwise view, by any method at the sole discretion of the University and without any additional advance notice to said user, any account and/or file stored on University computer resources. Should such a review take place, you will be given notice, as a courtesy only, of the results of said review within a reasonable time after the review is completed. While use of college computing resources for personal use is strictly forbidden, should you have materials for which you have reasonable expectation of privacy or which you consider to be confidential for any reason, you should retain those materials on a disk which can be secured as you would any other personal items or materials which you consider private in nature

Compliance with the GBLA Act

Overview: This section summarizes the Tusculum comprehensive written information security program mandated by the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act ("GLBA"). In particular, this document describes the Program elements pursuant to which the Institution intends to (1) ensure the security and confidentiality of covered records,

(2) protect against any anticipated threats or hazards to the security of such records, and (3) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers. The Program incorporates by reference the Institution's policies and procedures described below and is in addition to any institutional policies and procedures that may be required related to other federal and state laws and regulations, including, without limitation, FERPA.

Designation of Representatives: Tusculum's Chief Information Officer is designated as the Program Officer who shall be responsible for coordinating and overseeing the Program. The Program Officer may designate other representatives of the Institution, from other affected departments to oversee and coordinate particular elements of the Program related to their area. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officer or his or her designees.

Scope: The Program applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the Institution, whether in paper, electronic or other form which is handled or maintained by or on behalf of the Institution. For these purposes, the term nonpublic financial information shall mean any information (1) a student or other third party provides in order to obtain a financial service, (2) about a student or other third party resulting from any transaction with Tusculum involving a financial service, or (3) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

Elements of the Program:

- 1. Risk Identification and Assessment.** as part of the Program, to undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. The Program Officer will establish procedures for identifying and assessing such risks in each relevant area of the Institution's operations, including:
 - *Employee training and management.* The Program Officer will coordinate with representatives in Tusculum's [*Human Resources, Business and Financial Aid offices*] to evaluate the effectiveness of the Institution's procedures and practices relating to access to and use of student records, including financial aid information. This evaluation will include assessing the effectiveness of the Institution's current policies and procedures in this area, including (reference policies here)

- *Information Systems and Information Processing and Disposal.* The Program Officer will coordinate with representatives in Tusculum's [*Human Resources, Business and Financial Aid offices*] to assess the risks to nonpublic financial information associated with its information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. This evaluation will include assessing Tusculum's current acceptable use policy which can be found at <https://www3.tusculum.edu/is/appropriate-use-policy/> . The Program Officer will also coordinate with the specific Information Systems personnel responsible for assessing and monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.
- *Detecting, Preventing and Responding to Attacks.* The Program Officer will coordinate with the Institution's [*Department of Information Technology and other relevant units*] to evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Program Officer will delegate to the Systems Engineer, Webmaster/software analyst and Assistance Director the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the Institution.

2. Designing and Implementing Safeguards. The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The Program Officer will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

3. Overseeing Service Providers. The Program Officer shall coordinate with those responsible for the third party service procurement activities among the [*Department of Information Systems*] and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access.

4. Adjustments to Program. The Program Officer is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the Program.