TRANSYLVANIA UNIVERSITY

Acceptable Use Policy

Last Updated : January 2020

Transylvania University's Information Technology Department provides computer hardware, academic computer labs, network infrastructure and connection services in support of the educational mission of the University. Use of these services is a privilege. As such, it is the responsibility of all active members of the University community, including faculty, students, staff, authorized visitors, guests, and others for whom University technology resources and network access are made available by the University, to use these services appropriately and in compliance with all University, City, County, State and Federal regulations, or face possible revocation of such privilege.

Under that authority, Information Technology has established the following policies that are incorporated into and governed by the Student and Staff Handbooks. Please read carefully; failure to follow these guidelines may initiate appropriate disciplinary action for both students and employees.

General Policies

Computer facilities and accounts are owned by the University. Facilities include all computer equipment in labs and buildings on campus, and are available to Transylvania students, employees, authorized visitors and guests. Accounts include email, network, T-Net, Self-service and Moodle accounts, as well as any others issued by the University.

1. Please use common sense and think of others. Consideration of and respect for the rights, property (whether intellectual, electronic, or material), and time of others are central to the responsible use of computing facilities. Inconsiderate or malicious actions such as:
    a. stealing or using another's password or data;
    b. degrading the performance of the computer system;
    c. employing abusive or objectionable language;
    d. using another person's account or Crimson card;
    e. monopolizing the network with game play or excessive internet access;
    f. using printing services excessively and wastefully;
    g. interfering with another person’s use; and
    h. using technology to threaten or harm someone are rude, potentially dangerous and should be avoided.
2. The use of computers for class work takes precedence over personal use, such as email, Internet browsing, games, etc. When a lab is in use for a scheduled class, non-class members are not permitted to use the facilities.
3. Computing resources must be conserved. Do not waste them by sending prank messages, printing or downloading large files, sending chain mail, or other frivolous actions. Do not misuse or destroy equipment or resources.
4. Computing environments should be kept free of hazards to the equipment and free of annoyances to users. Eating and drinking are not allowed in any computer facility. Listening to music should be done only through a headset with volume low enough that others cannot hear. Transylvania University is a smoke-free campus.

5. Users are responsible for the tidiness of a facility. Do not leave items such as scraps of paper, outdated printouts, or other extraneous material in any computer lab.
6. All use of computing facilities must be authorized. Unauthorized access to labs outside of posted hours is not permitted.
7. Only authorized, licensed software may be used on University-owned computers. Other software may not be used on Transylvania equipment without permission.
8. Piracy of computer software is stealing and punishable by law, and will not be tolerated.
9. Each student and staff member will be provided a network account and official Transylvania Gmail email address (@transy.edu). This email address will be used for any official correspondence from the University. With this account, users can access network applications, save and retrieve documents from their Google Drive storage, and print to any of the lab printers. Visit the FAQ section of http://inside.transy.edu/it-help-desk/ for instructions about network and printing access and other useful information.
10. Any student may authenticate and connect to wi-fi on campus. Look for the wireless connection named “TUWIFI”. To register devices that do not support TUWIFI’s encryption, visit http://register.transy.edu
11. There is limited network storage on Transylvania’s servers. Since space is limited and is purged at appropriate times, users are encouraged to use their Google Drive storage space to store files, and to use Google Docs for creating and editing documents. Google Drive files can be accessed and edited on the web and via mobile apps from anywhere in the world, making it a convenient storage location. Always make backup copies of your important files. Saving copies to your personal computer, to a USB stick or to another cloud-based service are good ways to keep copies of your data.

12. The Registrar will notify Information Technology when students graduate. Graduating students' data and email accounts will remain in place until a set date at the end of the year that is communicated to students via email. At that time, all data and accounts for graduates will be erased. Graduating students are encouraged to make backup copies of their network files and email prior to graduating. The Registrar will notify Information Technology when a student withdraws from the University. Information Technology will then delete the account and erase any network files and email after a short period.
13. When in doubt, use common sense or do only what you have been specifically permitted to do. If there is a problem with equipment or you believe that someone is violating these guidelines, you may contact the IT director via email at itdirector@transy.edu.

Residential Network Policies

1. Any modification or unauthorized repairs to data wiring in the residence halls is considered destruction of University property. If you believe your outlet needs repair, contact the Helpdesk. Door access card swipes, security cameras and other technology equipment are university property; misuse or destruction of any equipment will be pursued by Transylvania's Department of Public Safety.
2. The Ethernet service may be extended from its wall outlet with an Ethernet patch cable up to 10 meters (33 feet) long. Extension of the Ethernet service from the wall outlet outside the room or apartment or using electronics equipment, such as routers or wireless access points, is not permitted.
3. Students must use UL approved equipment and materials, including computers, extension cords, etc.

4. Residents should understand that the network extended to student rooms is the property of the University and that the campus network administrators monitor and inspect network traffic for the purposes of ensuring both proper operation of the network and fair allocation of its resources.
5. Personal computers and devices may be connected to the network from the residence halls and other locations. Each student can connect to the network using wired or wireless connections where available. Look for the TUWIFI wireless network for most devices, or TUGUEST for game consoles and other devices, which must be registered first at http://register.transy.edu. For more details on how to register and connect devices, visit the FAQ on http://inside.transy.edu/it-help-desk/. If you encounter a Transylvania lab computer or device that needs to be registered or is asking to connect to the network, please contact the Helpdesk – DO NOT register it with your account information.
6. Information Technology will offer only limited support in connecting personal entertainment devices (such as video game consoles, digital video recorders, etc.) to the network. However, these devices are allowed.
7. The Residential Network may not be used to run computer servers that may potentially disrupt the operation of Transylvania's campus network. Specifically, no student's computer system may run a DNS server or DHCP server, including those available on routers and personal storage devices.
8. The Residential Network is a shared resource. Thus, network use or applications which inhibit or interfere with the use of the network by others are not permitted. For example, applications which use an unusually high portion of the bandwidth for extended periods of time, thus inhibiting the use of the network by others, are not permitted. Peer-to-peer or network file sharing programs are not supported by the network. Users may be asked to cease any system activity that directly or indirectly creates interference in the operation and administration of the network.

9. Network activity is monitored. Attempting to logon to or "hack into" any computer without an authorized account is forbidden. Trying to capture network traffic or using unauthorized IP numbers is prohibited. Students should not scan the network with the intent to compromise any other computer. Any student using an Ethernet connection in "promiscuous mode" or running a protocol analyzer to capture network data or passwords will have their access suspended immediately until further review by Information Technology and the Dean of Students.
10. A student may not use a hub or switch in their residence hall room to connect more than one wired device to the network. Wireless routers are unnecessary and may cause networking problems and are therefore prohibited. Any student found operating a router on campus will have their access revoked. Students may not use a personal wireless access point in the residence halls. Open wireless access is a security threat and may result in loss of internet access.
11. Residential Network connections may not be used for unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes (typically referred to as port scanning) and/or decrypt secure data.
12. Students are reminded that they should not use their computers in a hostile manner. Any activity with the purpose of denying another user the use of the network is harassment, which is a violation of the computing use rules.
13. Residential Network connections are subject to bandwidth shaping which may affect speed and performance in certain applications that are not deemed supported by the University.
14. Student IP addresses are automatically assigned by a DHCP server. Unless specifically directed by Information Technology, students should not make static IP assignments to their computer.

15. Use of Residential Network facilities to make copyrighted materials available on the network in a manner contrary to copyright or license agreements is prohibited regardless of the source of the copied materials. By federal law, the unauthorized distribution of copyrighted material, such as through peer-to-peer networks, may subject students to civil and criminal penalties. Information Technology will respond to all Digital Millennium Copyright Act requests as required by law, including providing the identification of student, faculty or staff users that are found to be in violation of the DMCA. Please see the United States Copyright Office site at http://www.copyright.gov and http://www.copyright.gov/help/faq/ for information on civil and criminal penalties for violation of Federal copyright laws. Legal alternatives for obtaining copyrighted material can be found at http://www.educause.edu/legalcontent/
16. The Residential Network may not be used to provide computer services or Internet access to anyone outside of the Residence Halls community for any purposes.
17. Residential Network access to the University's network services may not be used for commercial purposes, for personal financial gain, nor may the services be exchanged for money or any other thing of value. Advertising of the availability for sale of miscellaneous used personal property belonging to the resident is not commercial within the meaning of this paragraph.

Residents and their guests are expected to abide by the spirit of these policies and all guidelines mentioned herein when using these resources. Because technology evolves, new policies, procedures, and guidelines for ensuring that all users have the opportunity to pursue their academic and personal objectives unimpeded may be added as incidents warrant it.

Computer Security Policies

These policies apply to all active members of the University community, including faculty, students, staff, authorized visitors, guests, and others for whom the University has provided computer accounts: network, email, web, telnet, FTP, SSH, VPN, etc, and in-room Ethernet and/or wireless connections. Information Technology will provide security for these accounts by requesting that everyone follow the procedures listed below.

1. Transylvania University continues to install sophisticated computer networking assets for teaching, research, communication, and administrative purposes. Sensitive and private data and transmissions will be protected by appropriate equipment and administrative procedures. Information Technology will not tolerate abuse, ignorance, or lack of enthusiasm for computer security. If it is determined that an account is jeopardizing security, the account will be suspended immediately.
2. Users are responsible for what transpires on their computer. Each user must know and acknowledge the inherent risks of operating a computer connected to a network. If computing guidelines are violated, the user whose computer was used will be held responsible.
3. Users must not let others use their accounts or leave their password where others can find it.
4. Users should not leave their computer or a lab computer unattended when signed on, and should log off completely when they are finished computing.
5. Secure use of passwords is very important. Common words should not be used as passwords because they can be cracked within a matter of seconds. Please see the FAQ section of http://inside.transy.edu/it-help-desk/ for password requirements and guidelines.

6. Every six months, all users will be prompted to change their network password. These passwords must be unique, i.e., not previously used for the account. Students can change their password in a computer lab or via the password maintenance website at https://password.transy.edu. For more information on passwords, please visit the FAQ section of http://inside.transy.edu/it-help-desk/
7. If a student forgets their password or their password expires, they can reset it at https://password.transy.edu. Alternatively, they must apply in person to the Helpdesk (MFA 029) to have their password reset. Students must bring a picture ID with them when making this request. Requests to reset passwords cannot be honored over the phone or without a form of identification.
8. Every student who connects to the residential network must use some form of anti-virus software on their personal computer. Transylvania University recommends certain freely available anti-virus software programs. Please visit http://inside.transy.edu/it-help-desk/ for download information.

You are ultimately responsible for any use of your network connection, whether by you or a guest. Student violations of these policies will be handled through normal policy violation procedures established by the Transylvania University Student Handbook. Failure to comply with any of the above guidelines may result in sanctions consistent with the violation of University rules as presented in the Student Handbook which may include warnings, termination of in-room network services, forfeiture of housing, suspension or dismissal, other Residence Halls or University disciplinary action, and/or criminal prosecution. Faculty and Staff members are subject to the policy violation procedures established by the Transylvania University Employee Handbook. In accordance with University guidelines and/or court orders, network files and transmissions (data stored on university-owned computing equipment) may be subject to search and examination by system administrators. This is required to protect both the user and the integrity of computer systems such as those that are suspected to be involved in unauthorized use, abuse or misuse, or that have been corrupted or damaged. Questions about this policy or whether a particular activity would violate the policy should be addressed to the IT director via email at itdirector@transy.edu.

Vendor Access Policies

Access to computer systems and networks owned or operated by the University imposes certain responsibilities and obligations and is granted subject to the University policies, and local, state, and federal laws. Any vendor who does business with or for the University or acts as the University's agent with regards to provisioning, accessing, or otherwise utilizing technology resources is obligated to follow all relevant policies included in this document in addition to the following:

1. Vendor access must be uniquely identifiable and restricted to only the required resources.
2. Vendor must schedule maintenance (i.e. software patches, upgrades, etc.) with University IT personnel. Access to the University network and required resources will only be granted to Vendor during the maintenance window.
3. Vendor agrees to develop, implement, maintain and use appropriate administrative, technical and physical measures to preserve the confidentiality, security, and integrity and availability of all maintained or transmitted data.
4. Vendor agrees to only use University data, systems, resources, integrations, and access solely for the original purpose for which it was intended as defined in any contract that exists between the Vendor and the University.
5. Vendor will not mine or share University data with any third party without written permission from the University.

6. Vendor must report any security incidents directly to the appropriate University personnel.
7. Vendor agrees to comply with University policies and local, state, and federal laws as they apply to University systems and data.
8. Vendor must have a signed Non-Disclosure Agreement on record with the University.

Computer Support Policies

The staff of Information Technology is trained to repair many computer, printer and connectivity problems on University-owned equipment or network devices. Please follow these suggestions whenever you have a problem:

1. Check the Frequently Asked Questions section on http://inside.transy.edu/it-help-desk/.There is a good chance that the problem has already occurred and you may find instructions to fix the problem on your own.
2. Call, email or visit the Helpdesk (phone: x3593 or 859-281-3593; email: helpdesk@transy.edu) and identify the problem. The Helpdesk is located in 029, Michelle Fine Arts building (8:30am to 5pm Monday through Friday for walk-in, by phone from 8:30am to 5pm, additional hours via email). This procedure will allow Information Technology to initiate a support request, build a knowledge database problems and solutions, update the Frequently Asked Questions, and track the progress of the request.
3. The priority of these requests are as follows:
   a. campus wide network issue,
   b. network/technology issue affecting many users,
   c. individual mission critical computer failure,
   d. student network connectivity, email or software issue,

    e. faculty software or hardware issue,
    f. staff software or hardware issue,
    g. virus/spyware support for personal equipment owned by students.

4. Notify the IT director via email at itdirector@transy.edu for any other hardware or software support.

Support Scope Disclaimer

Information Technology personnel will support University-owned computers. On these computers, the staff will also support software purchased and installed by Information Technology personnel. However, Information Technology will not render support for individually-owned equipment except in two areas:

1. initial connection or problems with connecting to our network;
2. problems arising from malware. Information Technology no longer offers support for Windows 95, 98, ME, 2000, XP or Mac OS versions prior to 10.13. Linux support is limited but available on a best effort basis.

Students with other issues may seek assistance by calling the Helpdesk. IT staff will be happy to offer advice, suggest repair options, provide a list of students who may be willing to help, and indicate local computer/printer repair businesses.

Before any work is performed on a student's personal machine, a disclaimer form must be signed by the student. The Helpdesk will present this form at the time a student requests help.