

3. Circumventing the security of any St. Thomas system, including, but not limited to, identifying, exploiting, or attempting to exploit security flaws in same, or attempting to do so. Examples include: circumventing the computer registration processes and procedures for address assignment; creating or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain unauthorized access to any system. If you find a hole in the security of any St. Thomas system, notify Information Technology Services (ITS) staff immediately at (651) 962-1222.
4. Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, including, but not limited to: installing or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain unauthorized access to any system. If you find a hole in the security of any St. Thomas system, notify Information Technology Services (ITS) staff immediately at (651) 962-1222.
St. Thomas Exchange mail system and has not implemented responsible virus and spam controls, and thereby introducing a steady stream of infected messages to the St. Thomas system from within.
5. Refraining from any activity that will intentionally or negligently result in the unauthorized disclosure, modification, or deletion of any information stored on any St. Thomas system, including, but not limited to: installing or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain unauthorized access to any system. If you find a hole in the security of any St. Thomas system, notify Information Technology Services (ITS) staff immediately at (651) 962-1222.
altering ITS's level of access to a university system.
6. Using University systems or content (including subscribed library electronic databases) for personal gain, for commercial purposes, or for partisan, political purposes; for example, using University systems or content for commercial purposes, such as using University systems or content for profit with University resources in a manner not intended by the University, or using electronic mail to solicit advertising for products.
7. Making or using illegal copies of copyrighted software or data, here defined to include text, audio, video or other files of course materials, presentations, or other communications over University networks.

University. You may not place copyrighted material on any computer connected to the St. Thomas network, or use any computer connected to the St. Thomas network to store or use copyrighted material, unless you can demonstrate a teaching, fair use or research use exemption from copyright law, and you have obtained the appropriate permission from the copyright owner.

lawsuits and possibly to criminal charges.
8. Using University systems or content (including subscribed library electronic databases) for personal gain, for commercial purposes, or for partisan, political purposes; for example, using University systems or content for commercial purposes, such as using University systems or content for profit with University resources in a manner not intended by the University, or using electronic mail to solicit advertising for products.
9. Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, including, but not limited to: installing or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain unauthorized access to any system. If you find a hole in the security of any St. Thomas system, notify Information Technology Services (ITS) staff immediately at (651) 962-1222.
the network with either legitimate or illegitimate overloading thereof.
10. Sharing your username and password with others. Providing access to St. Thomas systems or networks to users who do not have an official St. Thomas account. Permission is granted to share your username and password with others only if you have obtained the appropriate permission from the administrator of the system or network.

11. Accessing or using network resources or devices without the express permission of Information Technology Services staff. This includes (but is not limited to) wireless access points such as the Apple AirPort hubs, switches, routers, printers, and protocol analyzers.

12. Abusing email.

email

Creating or deleting an electronic mailing list or user or machine in an electronic communication

Failing to comply with a request to stop emailing someone or to take them off a Distribution list

Sending all-campus email messages

Initiating or facilitating in any way mass electronic mailing (e.g., "spamming", "flooding" or "bombing") in excess of purposes of academic and business, and then only with the advice and consent of Information Technology Services

Taken together, these rules do not preclude sending non-work-related email to large lists of others. However, email should be treated as confidential and should be excluded from similar future mailings.

III Other University Codes of Conduct

Unauthorized use of course materials, especially technology resources. These policies are based on respect for the intellectual property of others.

IV Privacy

St. Thomas reserves the right to monitor and examine any and all network traffic on the university data network. Given the possible application of federal and state laws regarding confidential information, files, and data

and the School of Social Work will not be examined for content nor disclosed without the prior

your email or private files the St. Thomas reserves the right (as permitted by state and federal law) of designated ITS staff to log and examine any and all network traffic on the university data

network. St. Thomas systems, both central servers and desktops, whenever necessary, particularly but not exclusively in the following situations:

Policy), Information Technology Services will conduct an investigation. Investigations may involve other campus offices as needed.

For all digital communications (files or e-mail) are wanted as evidence on a non-computer-related university disciplinary matter (such as an academic dishonesty case or a sexual harassment investigation), ITS will provide those files on request of Dean of Students, the General Counsel, Academic General Counsel, the dean of the respective college, or the Assistant Vice President for Human Resources.

Unless the infraction involves potentially criminal behavior, ITS will make an effort to inform the individual that their files are being accessed.

ITS requests the data as part of an authorized investigation.

V. Enforcement

The University considers violations of acceptable use principles to be serious offenses. The University will take such action as is necessary to copy and examine any files or information resident on University network devices related to unacceptable use and to protect its network from system events that threaten or degrade operations.

In the case of minor infractions, ITS will make a reasonable effort to inform the individual of the incident. In the case of more serious infractions, ITS will make a reasonable effort to inform the individual of the incident.

In the case of a major infraction, ITS will make a reasonable effort to inform the individual of the incident. ITS will make a reasonable effort to inform the individual of the incident.

President of Human Resources, and other appropriate authorities, if necessary. ITS staff may take immediate denial of access to your account, loss of email privileges or removal of your system from the network. In cases involving violations of disciplinary offices will be given all information about an incident that ITS can collect. ITS will make a reasonable effort to inform the individual of the incident. ITS will make a reasonable effort to inform the individual of the incident.

VI. Further Information

If you have any questions about this policy, please contact the ITS Help Desk at (651) 962-6230 or the Office of the Dean of Students at (651) 962-6230.