3. [illegible] 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-[illegible]

4. Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, [illegible] St. Thomas Exchange system [illegible] implemented responsible virus and spam controls and thereby introducing a steady stream of infected messages to the St. Thomas system from within.

5. [illegible] 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, [illegible] for profit with university resources in a manner not [illegible] electronic mail to circulate 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 [illegible] over University networks. [illegible]

   University. You may not place copyrighted material on any computer connected to the St. Thomas [illegible] copyright or can demonstrate a teaching, fair or research exemption from copyright [illegible] [illegible] charges.

8. [illegible] person.

9. [illegible] network with either legitimate [illegible] overloading the [illegible]

10. Sharing your username and password with others. Providing access to St. Thomas systems or networks to users who do not have an off[illegible] ITS permission is prohibited. This includes providing user accounts on personal systems (i.e. -Anywhere passwords, or any such analog). If permission is granted, the administrator of that system is responsible for [illegible]

11. [illegible] 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

[illegible] ser 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\") except for purposes of conducting University 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 other users. However, mass mailings should be targeted to people who might reasonably be [illegible] to be excluded from similar future mailings.

III her University Codes of Conduct

[illegible] unauthorized use of course materials apply also to technology resources. These policies are based on respect for the rights and interests of others.

IV Privacy, Data Pr

[illegible] Given the possible applications of [illegible] 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 [illegible] St. Thomas systems, both central servers and desktops, whenever necessary, particularly but not exclusively in the following situations:

Policy), Information Technology Services will [illegible] involve other campus offices as needed.

For individual private files (including email) 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, Associate General Counsel, the dean of the appropriate college, or the Associate Vice President of Human Resources.

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

[illegible] uests 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 systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations.

In the case of minor infractions, ITS [illegible]

In the case of [illegible] ITS [illegible] ITS make a reasonable effort to [illegible]

President of Human Resources, and other appropriate authorities, if necessary. ITS staff may take [illegible] immediate denial of access to your account, loss of email privileges or removal of your system from the network. In cases involving violations of [illegible] disciplinary offices will be given all information about an incident that ITS can collect. ITS will [illegible] with all possible speed. The University's Data Security Policy contains more detailed information about the processes of investigations.

VI. Further Information

If you have questions about the [illegible] the ITS Help Desk at (651) 962-6230 or the Office of the Dean of Students at (651) 962-[illegible].