

University of Alabama at Birmingham

Department of Computer and Information Sciences

CIS IT Acceptable Usage Policy

In managing the limited resources available to the CIS community, we strive for fair, equitable and accountable use of the resources by all authorized users. This means that resource management and security are the responsibility of all users.

Note: For the purposes of this document, "CIS resources" refers to the network, computers, software, disk space, web space, printers, computer labs, special purpose hardware and any other equipment, resource or service owned or provided by the CIS department to its users.

Section 1. Authorized usage only

Accounts and access to CIS resources are issued to you and are to be used solely by you. You may not give anyone else access to these resources. If you do so, your account and/or access may be removed on a permanent basis. It is your responsibility to keep your accounts secure. If you are found using accounts or resources for which you have not been authorized, your own accounts may also be disabled permanently. This includes attempts to alter hardware, software or network configurations or connect personal equipment to the network without permission.

Section 2. Academic use only

CIS resources are provided for the sole purpose of supporting your academic computing needs related to the CIS academic program. CIS resources are not to be used for personal purposes unrelated to your CIS academic work. This includes the storage of files not related to your academic work. This policy extends to any web space which you may be granted. Excessive use of CIS resources for personal purposes may be treated as theft of services.

Section 3. Illegal activities

It is strictly forbidden to use CIS resources for illegal purposes. Examples of illegal usage include, but are not limited to, attempts to gain access to computer systems for which you are not authorized and the sharing or downloading of copyrighted material such as music, videos or books. Any illegal activities will be treated as attempted theft of services.

Section 4. File access

Even if permissions on another user's account permit you to view, copy, create or remove files, you may not do so without prior explicit permission from the owner of the file. Unauthorized file access will be treated as theft. This includes using other disk resources as a way to avoid disk space quotas.

Section 5. Email usage

Each student is responsible for reading all email from faculty and staff sent to both your CIS email address and your BlazerID email address (note that for new accounts the default behavior is to automatically forward CIS email to your BlazerID address). Announcements and policy changes announced by email to either of these addresses is considered formal notice and the student shall be held responsible for reading this information. You may not use CIS email resources to send unsolicited emails for the purposes of seeking employment, selling or buying services or merchandise or any other similar activity.