

Guidelines for Securing Electronic Information

Creating a secure environment for electronic information involves a multi-layered approach that requires the participation of all members of the campus community including the IT Security Manager, the system administrators and support personnel, and the end users. There are many potential threats to the security of your electronic data. Although some aspects of protection from these threats are the responsibility of IT professionals, some of the responsibility belongs to the users. The College has provided network resources to help you protect your work but there are additional steps you can and should take to ensure the safety of your electronic information.

Creating a Secure Environment

Creating a secure environment is a critical part of any effective security strategy. The following are steps you can take to create and maintain an environment that will help protect your electronic information.

Passwords

An important element in protecting your electronic information is implementing effective password protections. You should always use strong passwords that will not be easily guessed and keep your passwords secure. You should choose passwords that contain both alphanumeric and numeric or special characters. The password you choose should not be a word that is in the dictionary, your birth date, or any other easily guessed word or name. Include random characters, mix lower and upper cases, do whatever you can to develop a password that will not be easy to guess either by a person or by password-cracking software. Password-cracking software packages utilize dictionaries from many languages, so the dictionary rule isn't limited to English. One method for developing a password that is hard to crack but easy to remember is to take the first letter from each word in a long sentence to create a password that will not be in any dictionary.

Once you have established strong passwords on your accounts, you must be careful to keep them secure. Don't write your password on something that is easily found near your computer. Don't share your password with others. Don't make it easy for someone to access accounts or information that should be available only to you.

Virus Protection

The most well known of the security threats, infection by computer virus, can result in file corruption, installation of back doors into infected systems, and more. Virus infections can make it possible for intruders to take control of your computer, destroy your data, and possibly allow the system to be used to attack others. Anti-virus products are designed to help to prevent infection of your computer's operating system. The easiest way to protect your data from damage due to virus infection is to keep your anti-virus software current. All computers in the College installed by a member of the Computing Services staff are configured to automatically update virus definition files on a regular basis. If either your home or office system is not protected by anti-virus software, you can download and install anti-virus software free of charge from the OIT web site (www.helpdesk.umd.edu/virus/software.shtml). The University's license for VirusScan permits faculty, staff, and students to install the software on home computers, so you are encouraged to take advantage of this resource to secure your home computer. OIT also provides information about additional steps that can be taken to secure your computer and applications from virus infection (www.helpdesk.umd.edu/virus/other.shtml).

Limiting Physical Access

Many offices on campus are shared or are accessible by multiple people. The use of locking screensavers that require a password to access the machine can be helpful to keep people from accessing your machine while you are away from your desk for short periods of time during the workday. If there is a computer in your office that is used to store critical or sensitive data, you should limit the number of people who have access to it. Computers that store sensitive or valuable data, such as file servers, should be stored in locations that are not accessible by people who do not need direct physical access to them. Door locks for rooms that house critical systems should not be on the building master series and alarm systems should be considered in areas where security is vital.

Avoid Running Unnecessary Applications

Faults or bugs in the applications that are running on a computer often present security risks. If you are running a server to support shared research projects, a departmental or personal web site, or to keep track of sensitive administrative information, limiting the server to

running only those applications that are required will reduce the number of security risks associated with your server. For example, if you are running a Windows 2000 server and don't need to access it via the web, don't run the web server application. There is no need to leave open potential security holes in the system if you don't need the application.

If you are running a server, take the time to learn about how to secure the operating system. Most operating systems, including all versions of Microsoft Windows and most variants of UNIX (including LINUX), have security flaws in the basic installation package. Security updates need to be downloaded from the vendor and installed as soon as installation of the system is finished to fix these known problems. New patches and updates are released regularly to solve newly discovered security problems. Keeping the system up-to-date is critical. One reliable source for information about IT security is the CERT Coordination Center at Carnegie Mellon University (www.cert.org). You can sign-up for their mailing list to receive email notifications about security problems and solutions by visiting www.cert.org/contact_cert/certmaillist.html.

Cleaning Data from Old Hardware

One often overlooked element in securing your electronic information is to completely remove all personal data from your computer's hard drive when you replace your old computer. If your old office computer is being re-assigned for use in the department you need to be certain that any personal or sensitive data you have saved on the hard drive has been completely removed. This is also important if the department is disposing of the computer, as it is not unusual for such computers to be sold to other units on campus by Terrapin Trader. If Computing Services is installing your new computer you should work with them to ensure all sensitive data has been removed before the computer leaves your office. This security issue is also relevant when replacing your home computer. Security experts recommend that you physically destroy hard drives or wipe them clean before disposing of them. The best way to do that is to write over old information with new, useless data several times.

Ensuring Data Recoverability

Even in the most secure of physical environments it is important to do what is necessary to ensure that your data can be recovered if disaster strikes. There is always the risk of data loss due to hardware failure or

environmental emergencies such as fire or flood. The more important the data, the more steps you should take to ensure its recoverability.

Saving on the Server

All faculty and staff should be saving their work on the College files server. Not only is access to this space secured by password protection, data stored there is backed up nightly. Unlike data stored on your hard drive, files stored on the server are only accessible from your computer when you are logged into the server. Also, files you store on the server are backed up nightly and can be easily restored if needed.

Additional Security for Critical Data

For critically important data, such as research information that cannot be reproduced, you should store copies in multiple locations. One recommended strategy is to store a copy on the server and create separate copy on CD or other removable media that can be stored at an off-site location such as your home. This strategy results in no fewer than three copies in three separate locations: one on the server in a secured room in Francis Scott Key, one on the backup tape for the server in a secured room in A.V. Williams, and one on CD or other media at your home. By using this strategy you are protected from data loss and corruption due to hardware failure, fire or other environmental hazard, virus infection, or hacker attack.

Where to Go for Help

If you have questions or concerns about security either data you store locally or electronic information that is stored on departmental, College, or University servers, please contact Kathy Cavanaugh, Director of Computing Services, at extension 5-2116 or by email at kcav@umd.edu. Computing Services can make arrangements for security tests to be run on critical server or desktop machines to identify potential security risks. We can also schedule information sessions for departmental IT personnel to talk with IT security experts to help them establish policies and strategies for improving the security of the systems they support.