Policy on Protecting University Electronic Data

Securing Passwords

Faculty, staff, and students should protect their data and university data by practicing good password control and computer security practices. A secure password helps to prevent others from illegally accessing information.

Your login ID and password authenticate you as an authorized user of the University’s computing environment. A good password policy is key to the University’s overall systems security. You need to protect your own files and University resources by choosing a good password and protecting it.

Protecting Files and University Information

Backup of files on the network servers maintained by Computer User Services is the responsibility of Technology Access and Support; backup of local disks is the responsibility of the local user. Central backup will be scheduled to maximize user access while at the same time avoiding overtime and other extra operational costs. Backup tapes will be stored offsite to assure the ability to reconstruct the systems in the case of data loss.

The most important issue concerning computer security is the control of access to information and hardware. Only authorized users should have access to your computer and the ability to review, change, create, or delete information it contains. You must maintain the integrity, availability and confidentiality of the information as well as protect information from intentional or accidental modification, destruction, or disclosure. Data and applications on your internal hard disk may require additional security controls. Extremely confidential data is easily downloaded from main campus information systems, so caution should be take to ensure the security of any files stored on desktop systems.