

Computing and Information Services- Fred Miller, Chief Information Officer

Effective Date(s):

Title: 078.1 Information Systems Security

Applicable: Furman University (Students, Faculty and Staff)

Contacts: Computer Help Desk ext. 3277

Background

Computer systems are used to store, process and retrieve information that is private, confidential, and sensitive. Unauthorized access to, modification of, or falsification of such information is unethical and illegal. Within the scope of this document, the term “classified” shall collectively encompass any and all types (private, confidential, sensitive) of data stored in computing systems.

Policy

All programs and files within any computer system shall be considered classified and as such may be accessed only by those with a legitimate need to access such information and to whom permission has been granted by the person(s) responsible for its security. Exceptions to this policy shall be limited, but may include investigations to ensure the integrity or security of Furman University and its property, or to comply with law enforcement or legal requirements.

Guidelines

1. The Chief Information Officer has the responsibility for providing leadership in safeguarding the sensitivity, confidentiality and privacy of the programs and files. All users are expected to share this responsibility.
2. The absence of security protection on a file or resource shall not imply permission to access that file or resource.
3. Anyone placing classified information in a computer file, or designing systems to store and process classified information, must ensure that all reasonable measures to restrict access to that information are taken, and that all applicable laws and standards are followed.

4. Wherever feasible, each user of a computer system must be uniquely identified with a user account (to include a unique user identification and password) known only to that user. Each person assigned a user account will be responsible for all activity performed under to that username. Therefore, users should not share their passwords with others, should choose passwords that conform to the complexity standards set forth by the Computing & Information Services, and change them frequently.
5. Any new systems that are implemented must adhere to the requirement for unique user identification. Existing systems that rely on shared passwords should be phased out as quickly as possible.
6. Computing and Information Services will implement procedures which require users to choose passwords of a specified complexity, and to change them with a specified frequency.
7. Computing and Information Services and other departments that control or give permission for access to programs and data may be required to perform periodic audits to determine whether an individual's or a group's access to such programs and data is still appropriate.
8. Computing and Information Services must be notified immediately upon the termination of employment or student status of any individual that has access to Furman computing systems. Computing and Information Services staff will delete the accounts of such users. If continued access to data exists within those accounts, special arrangements can be made by supervisors.
9. This policy shall apply to all persons, including students, faculty members, staff members, and others.
10. This policy shall apply to all programs and data files within any computer system, whether the computer systems or files belong to a student, employee, administrative office or a third party such as a data processing customer.
11. Anyone who has knowledge of an attempt by anyone to violate this policy shall make known this violation to the Chief Information Officer.
12. Any person guilty of violating the security of any files or programs shall be subject to dismissal from the University and/or criminal charges.