Computer Systems Security

All servers (computer systems) at Converse University that have files and programs stored on them shall be considered confidential, private, and the property of the University. All users are given their own network storage space, Drive on Google Workspace, which they may use for storing document files as well as other directories assigned according to their needs.

1. Campus Technology is responsible for safeguarding the confidentiality and privacy of the programs and files on the servers and personal computers. This responsibility is to be shared by all users.
2. All faculty, staff, and students are given a unique user identification and password known only to that user. Each user will be held responsible for all activities attributed to that user identification. Therefore, no user shall share their password with others. Users are to use passwords that are difficult to guess and are to change their passwords frequently. Please refer to the Password Policy on https://my.converse.edu/ICS/Offices/Campus_Technology/Policies.jnz
3. The absence of security protection on a file or resource shall not imply permission to access that file or resource.
4. Everyone must ensure that all reasonable measures are taken to restrict access to files containing confidential information and that all applicable laws and standards are followed.
5. Campus Technology may implement security procedures that require users to choose passwords that are difficult to guess and can force a user to change them at a given interval.
6. Campus Technology must be notified by the Human Resources Office immediately upon the termination of an employee or by the Registrar's Office of a change in student status of any individual that has access to Converse University computer systems. This notification may allow for the deletion, disabling, or deprovisioning of the stated person's user account, thus protecting the security of Converse University computer systems and files.
7. These guidelines shall apply to all programs and data files within any computer system, whether the files belong to a student, faculty member, staff member, or any other member of the Converse University community.
8. Anyone who has knowledge of an attempt by anyone to violate these guidelines shall make known this violation to Campus Technology, who will take this information to the Vice President of Operations and Strategic Planning.
9. Any person guilty of violating the security of any files or programs shall be subject to disciplinary action by the University.

Password Policy

1.0. Purpose This policy establishes conditions for use and requirements for appropriate creation and management of Converse University system passwords.

2.0. Scope This policy applies to anyone who has a user account with Converse University.

3.0. Policy In order to protect the integrity of Converse University systems and users, it is necessary to create a password that would be difficult for someone to guess in an effort to gain unauthorized access to a user's Converse University account and systems.

A password must be:

1. Changed every 180 days
2. At least eight (8) characters in length
3. At least one (1) must be numbers
4. At least one (1) must be a capital letter
5. At least one (1) must be a lowercase letter.
6. At least one (1) special character (!@#$%^&*)
7. It must be significantly different from the previous password.
8. It cannot be the same as the user ID.

9. It cannot include the first, middle, or last name of the person issued the user ID.
10. It should not be information easily obtainable about the user. This includes license plate, social security, telephone numbers, or street address.
11. Safeguarded by not writing it down or storing it in a public place where others might acquire it.
12. Must never be communicated in person, email, or phone conversation.

Passwords should not be shared. However, Campus Technology Services may ask users for their passwords in order to complete certain user-requested services. The request will NEVER be unsolicited. Once the service is completed, the user should change their password.

All use of a Converse University account is to be performed by the person assigned to that account.

Account owners are held responsible for all activities associated with their accounts.

4.0. Services Changes to passwords can be completed at any time using https://www.converse.edu/password . If you have lost or forgotten your password, please visit the Campus Technology Help Desk in Kuhn or go to .