Communication Disorders Clinic
Computer Systems Security Policy

Goal

To provide a reasonable and acceptable level of security for the users of computer and networking systems, to use reasonable effort to protect data from accidental or deliberate tampering or removal, and to prevent access and use of computer systems and files by unauthorized persons or entities.

This policy covers the use, management, and administration of computer user accounts for identification and authentication and for regulating access to computer and networking systems. For the purposes of this document, "*Login Name*" refers to the account name assigned to the computer user by the University. Accounts are granted to enrolled students (current and future terms), faculty, staff and retirees. Any exceptions are handled separately, documented and tracked as necessary.

User Responsibilities

The account owner is responsible for all actions and functions performed under his/her account. Unauthorized access to university accounts is prohibited. To preserve the security of university computer accounts, users are expected to act responsibly as follows:

- Users may never share their computer accounts.
- Users may not disclose their passwords to others.
- Users should log off and/or secure workstations when not in use.
- Users should secure their workspace area when not in the office.
- Users will be required to change their passwords frequently (every 90 days, minimum).
- Passwords should not be set to anything that is associated with the user.
- Passwords must contain at least six characters using a combination of letters and numbers.
- Passwords should not be displayed or posted where unauthorized personnel can discover them.
- Suspicious systems activity should be reported to the systems administrator immediately.
- Users should refrain from embedding or hard-coding passwords into any system

System Administration

- Identify each user with a unique Login Name.
- Enable timed logout feature for extended session inactivity periods.

Account Maintenance

- Revoke or delete accounts with no activity for a period greater than 14 months.
- Promptly disable accounts when a user is no longer eligible to have them.
- A limit of 3 to 5 unsuccessful attempts is strongly recommended. Disable the account when the limit is reached.
- Maintain audit logs to record login activity. Periodically review audit logs to detect suspicious login attempts.
- Restrict account and password management functions to authorized staff.

- Maintain accurate records of to whom, for what reasons, and for what functions such access is granted.

Password Management:

- Set minimum password length to 6 characters, using a combination of letters and numbers.
- Passwords should not be set to anything that can be readily associated with the user such as: birthdays, first or last names, telephone numbers, etc.
- Force password changes, where possible, during first time login.
- Require password changes minimally at the following intervals: system administrators, 30 days; users, 90 days.
- Mask input of all passwords.
- Encrypt passwords during storage and transmission over networks.
- Refrain from embedding or hard-coding passwords into any system.