University of Colorado
Anschutz Medical Campus

Administrative Policy

Title: **Acceptable Use Policy**

Source: **Graduate School**

Prepared by: **Jordan Schiefer**

Approved by: **David Engelke**

Effective Date: **01/01/2020**

Applies: **All staff members in Graduate School, including full time staff, part time staff, and temporary staff (includes contractors, temps and students)**

A. Introduction

The purpose of the acceptable use policy is to establish processes and guidelines to all staff members in **Graduate School**, including full time staff, part time staff, and temporary staff (includes contractors, temps and students). The user shall only be granted access to the minimum necessary data that they require to perform their duties.

B. Policy Statement

The use and access of **Graduate School** information systems is restricted to appropriately identified, validated and authorized individuals. The following subsections outline the requirements for gaining access to **Graduate School** information systems.

C. Workstation Use and Security

a) Each workforce member must use a unique user name and strong password to access their workstation and subsequent data both locally and via server.

b) Computer workstations accessing FERPA data must maintain security configurations that restrict access to data to only those workforce members that have been legitimately granted access. Recommended security configurations include, but are not limited to:

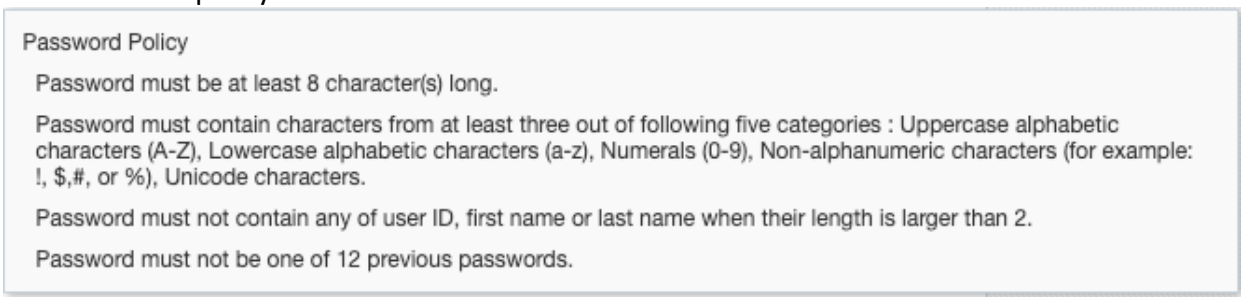
   i) Enabling a password protected screen saver

   ii) Setting computers or applications to automatically terminate a computing session after a set period of idle time

iii) The use of campus standard anti-virus products
iv) Applying security patches to computer software applications and operating systems
v) When Anschutz stores, shares, and syncs work files internally or externally, it is important that the confidentiality, integrity, and availability of that data be preserved. OneDrive can be used to store, share, and sync work files internally or externally with the following guidance.
   a) https://www1.ucdenver.edu/offices/office-of-information-technology/software/how-do-i-use/onedrive
   b) https://www1.ucdenver.edu/docs/default-source/offices-oit-documents/how-to-documents/onedrive-staying-secure.pdf?sfvrsn=668bb7b8_4

D. Unit Responsibilities

a) Unit educates their workforce members on the unit's specific procedures and requirements as necessary. Training requirements for gaining access to Unit Information Systems are listed below.
   i) Required skillport courses in UCDAccess once beginning employment term:
      a) CU: Information Security and Privacy Awareness (u00063)
      b) CU: FERPA (u00049)
   ii) Per OIT's Active Directory compliance, users must create a password to meet OIT's standards for mail, AD, domain access, etc. This password is changed each quarter, and must be different from the previous 12 passwords. See password policy below:


Password Policy

Password must be at least 8 character(s) long.

Password must contain characters from at least three out of following five categories : Uppercase alphabetic characters (A-Z), Lowercase alphabetic characters (a-z), Numerals (0-9), Non-alphanumeric characters (for example: !, $,#, or %), Unicode characters.

Password must not contain any of user ID, first name or last name when their length is larger than 2.

Password must not be one of 12 previous passwords.

E. User Responsibilities

a) CU Denver|Anschutz workforce members must observe the CU Denver Information Systems' Appropriate Use Policy (AUP) which outlines expectations regarding the ethical and permissible use of CU Denver|Anschutz computing resources.
b) CU Denver|Anschutz workforce members must follow the provisions of the CU Denver|Anschutz OIT Security Computing policy in regard to guarding against, detecting, and reporting malicious software
c) CU Denver|Anschutz workforce members shall not attempt to alter audit records or avoid accounting for computing services. (See CU Denver Information Systems' Appropriate Use Policy (AUP))

d) CU Denver|Anschutz workforce members shall not use CU Denver|Anschutz resources to develop or execute programs that could infiltrate the systems or alter the software components of the workstations.
e) CU Denver|Anschutz workforce members must follow the Portable Media Security Policy. Portable media can include, but is not limited to, laptops, mobile devices such as personal digital assistants (PDAs) or other types of wireless handheld devices, USB flash drives, memory sticks, and any other portable device used to store or transport data.
f) CU Denver|Anschutz workforce members must follow the Visitor Control guidelines outlined in the Access Control Policy when visitors are on-site.
g) All members of the CU Denver|Anschutz workforce are reminded to wear their badges while on University property.

F. Action

All suspected policy violations, workstation compromise, virus infections, and other conditions which might jeopardize CU Denver|Anschutz information systems, data, or business must be immediately reported to the OIT Security Office.