University of Colorado
Anschutz Medical Campus

Administrative Policy

Title: **Access Control 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 access management section is to establish processes to control access and use of Graduate School information resources. Access management incorporates Role Based Access Controls (RBAC), privileged user access, access definitions, roles, and profiles. The user shall only be granted access to the minimum necessary information 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.

Additional Resources:

- **OWASP Access Control Cheat Sheet**
- **Access Control in Software Development**
- **OWASP Cheat Sheet Collection**

C. Access Control Procedures

Systems must develop, adopt or adhere to a formal, documented access control procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

a) **Account Management-User Access**

- Access management to information systems to be granted (ex. passwords, etc)
  - Graduate School relies on OIT authentication systems (AD, etc.) to authorize users of the University of Colorado Denver|Anschutz computing resources.
  - The GS IT Admin adjusts user permissions based on requests of their supervisors for server shares.
  - Default passwords are to be changed or disabled, replaced with secure passwords
- Responsible party for monitoring and reviewing access rights
  - GS IT Admin reviews access rights upon every new hire, every termination, and at a bi-annual schedule, after each semester.
- Access and use of systems resources and subsequent monitoring (project space/ application/storage, remote access, mobile devices, etc.)
  - Systems are audited internally every semester, reviewing security groups and users on GS domain
  - Users with edit access on web pages are also reviewed
  - Remote access is limited to access via GlobalProtect VPN hosted by OIT
- Off-boarding process for users that are no longer working on the project, terminated, or have a change in job role.
  - User's supervisor notifies and submits request to GS IT Admin
  - GS IT Admin removes user from security groups, using the concept of least privilege, or removing altogether if terminated
- GAIA access has always been granted to Departmental and Program administrators upon request (desire to use GAIA for data storage and reporting). Users are only given as much access as required (typically level 4 for admins). Faculty are also given access, but with a lower level (2).

b) Workstation Use and Security

i. Each workforce member must use a unique user name and strong password.

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

1. Enabling a password protected screen saver;
2. Setting computers or applications to automatically terminate a computing session after a set period of idle time;
3. The use of campus standard anti-virus products;
4. Applying security patches to computer software applications and operating systems.

D. Physical Access

a) Facility Access Controls
   i. Facility security consists of:
      1. On both campuses, the Graduate School is locked down outside the hours of 8am-5pm, requiring approved card access.
      2. Upon entry, each office and subsequent equipment is further protected by physical lock-and-key.

b) Access Control
   i. Access determinations must be based on the workforce member's role or function within the unit. Determinations of access should take into account at what time(s) access will occur and under what conditions.
   ii. Unit managers or supervisors will work with the Badging and Security Services Security Badging Office/Electronic Security Department to request and recommend access for each member of the unit workforce. For specific access forms, contact the Badging and Security Services Security Badging Office/Electronic Security Department at (303) 724-0399.
   iii. If a workforce member's access needs change or end, the unit manager or supervisor must work with the Electronic Security Department to modify or terminate the member's access.
      1. Anschutz Medical Campus
         a. Associate Dean works with Electronic Security Department to enable/disable access based on new employment, termination, or move within CU.
         b. The supervisor or HR advisor submits the request to Associate Dean, who funnels all requests accordingly.
      2. Denver Campus
         a. Supervisor requests access card via Facilities Management and turns it in upon termination or relocation outside of GS.
   iv. The unit manager or supervisor must ensure that access is limited to what is appropriate for the workforce member's job function.

c) Validation Procedures

i. Once an individual's facility access has been determined and recommended by the individual's supervisor, validation of identity is performed by the Badging Office.
ii. All members of the CU Denver workforce are reminded to wear their badges while on University property.

d) Maintenance Records
   i. The Badging and Security Services Security Badging Office/Electronic Security Department is responsible for maintaining records on all installations, repairs, or replacements of access control devices at a building or campus-level.

E. User Responsibilities

a) Graduate School educates their workforce members on the Graduate School's specific procedures and requirements as necessary. Each Unit will educate users on the Acceptable Use Policy specific to their environment.
   i. See Acceptable Use Policy, section E
b) Please explain your unit's training requirements for gaining access to Graduate School Information Systems.
   i. See Acceptable Use Policy, section D

F. Graduate School Access Review

Please explain how access is reviewed.

Review accounts on a periodic basis, but no less than every six months.

G. Graduate School Policy Review

Review and update policy and procedures on an Annual basis.

H. Documentation Retention

All unit procedures, documentation of decisions made, information system activity reviews, and investigations conducted pursuant to this policy must be retained for a period of no less than six (6) years from the date the policy was last in effect or from the date the decision or investigation was made.

I. Revision History

Revision Number	Summary of Revision	Revision Author	Date	Accepted By
1	Initial Draft	Jordan Schiefer	11/19/2019	