ALBERTA COLLEGE OF ART + DESIGN

ACAD

INFORMATION TECHNOLOGY USER ACCESS PROCEDURE

PROCEDURE #:	600.01.01.01
SECTION:	Computing + Technical Services
RELATED POLICY:	600.01.01 Acceptable Use
ORIGINAL APPROVAL DATE:	April 1, 2011
LATEST APPROVAL DATE:	**April 24, 2018**
APPROVING AUTHORITY:	Original signed by President + CEO

Purpose

This document outlines the process of granting, managing, and removing authorized users' access to ACAD information assets. The procedure helps prevent unauthorized access, fraud, theft, and misuse of ACAD information assets.

Scope

This procedure applies to all ACAD information assets including wireless and remote access, security devices, and all authorized users.

Definitions

Authorized Users: Includes students, staff, faculty, employees and third party users such as contractors, consultants, temporary users, suppliers and service providers.

Information Assets: Includes all business applications, infrastructure related applications, databases, networks, operating systems, technology infrastructure, intranet, email, and hand held devices, wireless devices, security devices, files, and data.

Information Asset Owner: The ACAD Employee responsible for the management of an Information Asset.

User Access Administrator (UAA):	Information Technology Personnel responsible for recording and tracking IT asset access privileges assigned to each Authorized User. The UAA cannot also be a CAA.
Computing and Technical Services (C+TS):	Shall regularly monitor network performance, traffic flow and resource utilization. Where disruptions point to a violation of access guidelines, an investigation and corrective action shall be undertaken to preserve and protect the information assets and to restore acceptable access protocols.

Procedure

1 Authorization for User Access Maintenance

1.1 Creating User Access

1.1.1 A Faculty and Staff new hire's access is initiated by Payroll sending an email on behalf of the hiring manager to Helpdesk. A tracking ticket is created. The email contains the hiring manager name, charge code, start date, position title and employee name. Ending date is indicated for Temporary and Casual hires.

1.1.2 Student accounts are bulk generated each term from lists created from Banner.

1.1.3 Contractor accounts, if necessary, are requested by the contracting department and are unique to each contract with the minimum access needed to fulfill their contract. Ending date is indicated for contractor hires.

1.1.4 Role-based access is granted to a new user based on their position title.

1.1.5 A default access profile, identical for all identical position titles, is maintained in C+TS. The CAA prepares a new profile for a new user matching the default for their position.

1.1.6 The UAA records the new authorized user name, position, email address and IT asset access privileges. If the authorized user is Temporary, Casual or a Contractor, the end date is also recorded.

1.2 Changing User Access

1.2.1 The Information Asset Owner and/or Requestor submits the User Access Request to the Helpdesk via email. A tracking ticket is created.

1.2.2 The changes can be temporary for an individual or permanently changed to the access for that position title. Temporary changes in access for an individual must have a time limit for review and continuation or deletion and restoration of the default access.

1.2.3 When the change is to the role based access for the position, all staff with that position title will have their access changed at the same time.

1.2.4 When the requestor and the asset owner are different, the Information Asset Owner must also approve the Helpdesk tracking ticket. Their approval is accepted by being added to the Helpdesk ticket and submitting their approval message within the ticket.

1.2.5 After the changes have been made, the CAA updates the ticket which sends an email to the user and Requestor that the change has been completed.

1.2.6 The UAA records the changes to the authorized user name, position, email address or IT asset access privileges. If the authorized user is Temporary, Casual or a Contractor, the end date may also be updated. If the access change is temporary, the end date for the access change is recorded.

1.2.7 CAAs may not change their own access privileges.

1.3 Deleting/Disabling User Access

1.3.1 Changes to the status of a user whose employment with ACAD has been terminated, shall be reported by the user's manager or by payroll on behalf of the user's manager via an email to Helpdesk.

1.3.2 The user's manager shall indicate how the user's email account, local computer files, and personal network files shall be handled. Without instructions, the email and network files are archived and a decision request is escalated in the user's department.

1.3.3 The CAA then disables all access privileges and accounts of the terminated user and updates the ticket which sends an email to the Requestor that the change has been completed.

1.3.4 The UAA removes the authorized user name, position, email address and IT asset access privileges. If the authorized user is Temporary or Casual, the end date is also removed.

1.3.5 The user's local computer profile shall be wiped by CAA before the computer is assigned to a new user.

2 Authentication

2.1 User ID

2.1.1 Users shall be provided a unique user ID to access information assets, applications and infrastructure. The use of group IDs or generic IDs shall only be permitted where they are necessary for business or operations reasons and shall be approved by the MIO and Information Asset Owner.

2.2 Password

ACAD's password shall:

2.2.1 Comprise a minimum of eight characters and contain at least 3 of the following:

- Upper case letters
- Lower case letters
- Numbers
- Printable symbols ~!@#$%^&*_-+=\|()\{}[]:;"'<>?/,.

2.2.2 Be changed at next login when an interim or temporary password is assigned

2.2.3 Be changed annually

2.2.4 Not contain the user name

2.2.5 Not be re-used (i.e., password reuse within 6 generations is automatically prevented)

2.3 Account Lockout

2.3.1 MIO will run an activity report every 4 months and disable inactive accounts that exceed 4 months of inactivity.

2.3.2 The user's account shall be locked out automatically after 5 invalid logon attempts. Only a CAA can manually unlock the account. Accounts shall automatically be re-enabled after 10 minutes of inactivity.

3 Access Privileges

3.1 The access privilege to business applications shall be on a "Role-Based Access" principle. ACAD Systems' access privileges shall be enabled based on the role of the employee.

3.2 Information asset access entitlements and controls are established by the Information Asset Owner.

3.3 CAA shall grant access to roles.

3.4 The Director, C+TS directs the UAA to maintain the list of users with the details of the access privileges granted for each information asset. The list represents the current state snapshot of all approved access privileges.

3.5 Any required new roles shall go to the ITSC for approval before granting access.

4 Third Party Access

The third party user access procedures follow the same process as described in this document with some additional procedures, as follows:

4.1 For every third party user, ACAD shall identify a point of contact within the College to ensure that the third party user is in compliance with ACAD Information Security Policy.

4.2 Expiration date for every third party user account shall be defined in accordance with the contract. Network and business application access if possible, shall be configured to expire automatically on a pre-determined end date in line with the terms of the contract. The CAA shall ensure the account is disabled as soon as the contract expires.

4.3 Third party users shall sign a Confirmation of Understanding of Conduct and Behavior Agreement, accepting and agreeing to at least the following:

- Procedure 200.29.: Information Technology - Acceptable Use
- Procedure 400.21.: Disclosure Protection
- Procedure 400.02.: Respectful Workplace

- Procedure 400.20.: Conflict of Interest
- Procedure 400.19.: Code of Conduct

4.4 User Responsibilities

Users must:

4.4.1 Keep passwords confidential (never share your password);

4.4.2 Change passwords at prescribed intervals or whenever there is any indication of possible system or password compromise;

4.4.3 Select complex passwords with minimum length (as specified above) which are:

- easy to remember;
- that cannot be guessed easily (i.e. don't use personal information like family names, telephone numbers, or date of birth);
- not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);
- free of consecutive or identical, all-numeric or all-alphabetic characters;

4.4.4 Not use the same password for ACAD and non-ACAD purposes

5 Reviewing and Monitoring

5.1 Three times per year (fall term, winter term, spring or summer term) review of users' access to infrastructure related applications shall be performed by the MIO to ensure that all network & operating systems active accounts are appropriate.

5.2 Three times per year (fall term, winter term, spring or summer term) the major Information Asset Owners shall review business application users' access to confirm the appropriateness of their users' access privileges. The UAA provides a snapshot or current access for each user in each department.

5.3 Unusual access or activity on key business and infrastructure related applications shall be reviewed by MIO to ensure access integrity is maintained.

Roles and Responsibilities:

6 Requestor: User and or user's manager responsible for requesting the following:

- Appropriate access privileges for a new user
- Changing the access privileges of an existing user
- Deleting the access of terminated user

6.1 User's immediate supervisor or his delegate is the approver of the request (users may not authorize their own access request).

7 **Manager, Infrastructure + Operations (MIO) –** responsible for the overall operation, management and periodic review of all authorized users' access privileges on the network.

8 **Computer Accounts Administrator (CAA) –** Information Technology Personnel responsible for the creation, administration, and deletion of user accounts.

9 **Information Asset Owners –** Assigns and manages access to their Information Asset.

10 **User Access Administrator (UAA) –** Information Technology Personnel responsible for recording and tracking IT asset access privileges assigned to each Authorized User. The UAA cannot also be a CAA.

11 **Computing and Technical Services (C+TS)** shall regularly monitor network performance, traffic flow and resource utilization. Where disruptions point to a violation of access guidelines, an investigation and corrective action shall be undertaken to preserve and protect the information assets and to restore acceptable access protocols.

Related Documents:

ACAD Information Security Policy

Administrator Access Guideline

Role Based Access Matrix (All Staff Roles.xls)

ACAD.ca Access Matrix.xls

Procedure 600.29.: Information Technology - Acceptable Use

Procedure 400.21.: Disclosure Protection

Procedure 400.02.: Respectful Workplace

Procedure 400.20.: Conflict of Interest

Procedure 400.19.: Code of Conduct

Procedure 600.02.: Copyright

Procedure 600.14.: Social Media

Procedure 600.15.: Website