IT: USER ACCESS PROCEDURE

Procedure Type:	Institution	**Initially Approved:**	April 01, 2011
Procedure Sponsor:	VP Administration	**Last Revised:**	August 11, 2020
Administrative Responsibility:	Computing & Technical Services (CTS)	**Review Scheduled:**	August 2025
Approver:	President and CEO		

A. INTENT

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

B. SCOPE

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

C. PROCEDURES

1. Authorization for User Access Maintenance

1.1 Granting User Access

a. A Faculty and Staff new hire access request is initiated by Human Resources sending an email on behalf of the hiring manager to the AUArts Helpdesk, whereby a Helpdesk ticket is automatically created:
   i. The email contains the hiring manager name, charge code, start/end date, position title and employee name.
   ii. An end date is required for Temporary and Casual hires.

b. Student accounts are bulk generated each term from lists created from AUArts Student Information System.

c. Contractor accounts are requested by the contracting department and are unique to each contract with the minimum access needed to fulfill their contract
   i. An end date is required for all Contractor hires.
   ii. See section 4 for additional requirements when hiring Contractors.

d. Privilege-based access is granted to a new user and is based on the approval of the information asset owner(s).

1.2 Managing User Access

a. The Information Asset Owner and/or Requestor submits a User Access Request to the Helpdesk via email.

b. Only the Asset owner can approve access to the asset.

c. Changes to access can be temporary or permanent, depending on the nature of the access needs.
    i. Temporary changes in access for an individual must have a time limit for review and continuation or restoration to the default access.
d. The CAA records the changes to the username, position, email address or asset access privileges.
    i. If the user is Temporary, Casual or a Contractor, the end date may also be updated.
    ii. If the access change is temporary, the end date for the access change is recorded.
e. CAAs may not change their own access privileges

1.3 Removing User Access

a. Upon end of employment or end of studies, the user's access termination request must be reported immediately via email to the Helpdesk by either HR or the user's Manager.
b. The Helpdesk email request shall indicate any special handling requirements for the user's email account, local computer files, and network files.
c. Without special handling instructions, accounts will be deleted, along with any email and personal network folders and files
d. The CAA will disable all access privileges and accounts assigned to the terminated user and will update the Helpdesk ticket, informing the Requestor that the change has been completed.
e. The user's local computer shall be wiped by CAA before the computer is assigned to a new user.

2. Authentication

2.1 User ID's (individual, generic, shared, systems)

a. Users shall be provided a unique user ID to access information assets, applications, and infrastructure.
b. The use of generic, shared, or system IDs shall only be permitted where they are necessary for business or operations reasons and shall be approved by the assigned owner of the account.

2.2 Passwords

a. Are comprised of a minimum number of characters and symbols, including upper and lower case.
b. Initial passwords are to be changed at next login when an interim or temporary password is assigned.
c. Change passwords at the prescribed intervals or whenever there is any indication of a possible system or password compromise.
d. Are changed on a scheduled basis at a regular interval.
e. Are kept confidential (never share your password).
f. Cannot contain the username.
g. Cannot be re-used.
h. Do not use the same password for AUArts and non-AUArts purposes.

2.3 Account Lockouts
   a. A user's account shall be locked out after a set number of failed logon attempts resulting from a suspicious activity alert, and/or when the asset owner deems the account is no longer needed.

2.4 Elevated System and Service Accounts
   a. Shall only be used for the business purpose for which they were designed and are not intended to provide elevated access for non authorized purposes.
   b. Elevated system or service accounts must be approved by the Director of Computing + Technical Services.

***Note:** some systems or applications may require variations identified in this procedure, subject to approval.

3. Access Privileges

3.1 Access shall be granted using a "Privilege-Based Access" principle, through approval of the Information Asset Owner.
3.2 Information asset access entitlements and controls are established and reviewed by the Information Asset Owner.
3.3 A CAA shall only assign privileges after receiving approval from an Information Asset Owner.
3.4 The Director of Computing + Technical Services ensures an audit of access privileges is conducted by Information Asset Owners for their in-scope information assets.
3.5 The audit is reviewed and approved by the Information Asset Owner.

4. Third Party Access

Third-party user access follows the same process as described in this document with some additional controls.

4.1 For every third-party user, an AUArts Hiring Manager shall ensure that the third-party user is in compliance with AUArts Information Security Policy.
4.2 An expiration date for every third-party user account shall be defined in accordance with the contract.
4.3 The Hiring Manager is responsible for ensuring third party users sign a Confirmation of Understanding of Conduct and Behavior Agreement, accepting and agreeing to at least the following:
   a. Policy: Computing + Technical Services - Acceptable Use.
   b. Policy: Code of Conduct.
   c. Procedure: Public Interest Disclosure Policy.
   d. Procedure: Respectful Workplace.

5. Reviewing and Monitoring

5.1 User access reviews shall be performed regularly to ensure active accounts are appropriate.
5.2 Unusual access or activity on key business and infrastructure related applications may be reviewed to ensure access integrity is maintained.

6. Roles and Responsibilities

6.1 The Director of Computing + Technical Services is accountable for the overall operation, management framework and periodic review of all authorized users' access privileges on the network.
6.2 Information Asset Owners are responsible for approving and reviewing access to their Information Assets.
6.3 Computer Accounts Administrator (CAA) are responsible for the creation, administration, and deletion of user accounts.
6.4 Computing and Technical Services (C+TS) are responsible for regularly monitoring network performance and taking corrective action to preserve and protect the information assets.
6.5 All user account holders are responsible for adhering to the requirements of this policy and any related policies or procedures.

D. DEFINITIONS

Authorized Users:	Students, staff, faculty, employees, and third-party users such as contractors, consultants, temporary users, suppliers, and service providers
Information:	AUArts data in any form or media, including databases and computer files, which is collected, transmitted, stored or maintained on AUArts' information systems or elsewhere
Information Systems:	AUArts' Information Technology (IT) networks, systems and applications
Information Assets:	Information and information systems
Information Asset Owner:	The AUArts Employee responsible for the management of an Information Asset
Computer Accounts Administrator (CAA):	Information Technology Personnel responsible for the creation, administration & deletion of user accounts

E. RELATED POLICIES

- Code of Conduct Policy
- Public Interest Disclosure Policy
- Copyright Policy
- Access to Information and Protection of Privacy Policy
- Acceptable Use Policy
- Social Media Policy
- Website Policy
- Respectful Workplace Policy

F. RELATED LEGISLATION

- Alberta “Freedom of Information and Protection of Privacy” Act

G. REVISION HISTORY

Date (mm/dd/yyyy)	Description of Change	Sections	Person who Entered Revision (Position Title)	Person who Authorized Revision (Position Title)
07/31/2020	Template Update and Content Revisions		Director, CTS	
04/24/2018	Revisions			