INFORMATION TECHNOLOGY: USER ACCESS POLICY

Procedure Type:	Institutional	**Initially Approved:**	February 3, 2026
Procedure Sponsor:	Vice President, Finance and Operations	**Last Revised:**	February 3, 2026
Administrative Responsibility:	Information Technology (IT)	**Review Scheduled:**	February 2027
Approver:	President and CEO		

A. PURPOSE

This policy provides a framework for managing secure user access to Alberta University of the Arts' (AUArts) Information Assets.

It ensures that user access is authorized, auditable, and revocable to protect sensitive data and maintain security.

B. SCOPE

This policy applies to all employees, faculty, third-party contractors and students that access or manage AUArts' Information Assets (collectively "Authorized Users").

C. POLICY

1. GENERAL

1.1 Each user shall be provided a unique user ID.
1.2 Access must be granted based on the principles of least privilege.
1.3 All access must be formally approved.
1.4 Access must be revoked immediately upon termination or role change.
1.5 Access for third-party users must be approved, monitored, and governed by contractual agreements.
1.6 Access shall only be used for the purpose for which it was designed and is not intended to provide access for non-authorized purposes.
1.7 Remote access must be appropriately secured and granted only to authorized users.
1.8 No user, even if they have the administrative privileges to do so, may change their own access privileges.
1.9 AUArts reserves the right to revoke the system privileges of any user at any time.

2. PASSWORDS

2.1 Passwords must be at least twelve characters long and contain a combination of uppercase letters, lowercase letters, numbers and symbols.
2.2 Passwords cannot contain the username.

2.3 Passwords must not be based on a user's easily accessible information or that of the user's family members, pets, friends or co-workers.
2.4 Initial passwords must be changed at next login when an interim or temporary password is assigned.
2.5 Passwords are changed on a scheduled interval basis, as determined by Information Technology, and may be adjusted from time to time based on the threat environment, system risk, and evolving industry best practices. Passwords must be changed whenever there is any indication of a possible system or password compromise.
2.6 Passwords are kept confidential (never share your password).
2.7 Users must not use the same password for AUArts and non-AUArts purposes.

3. ACCOUNT LOCKOUTS

3.1 A user's account shall be locked out:
a) after a set number of failed logon attempts
b) if a suspicious activity alert is received
c) when the Information Asset Owner deems the account is no longer needed
d) for non-payment of Student Fees
e) after 60 days of inactivity
3.2 Access rights shall be modified or removed in accordance with information security, Human Resources, and other organizational policies and procedures. The user's identity must be verified before a disabled account can be reenabled.

4. TWO-FACTOR AUTHENTICATION (ALSO CALLED MULTI-FACTOR AUTHENTICATION)

4.1 Two-factor authentication will be implemented requiring use of at least two distinct factors (e.g., password and authenticator) for all remote access, privileged accounts, and access to sensitive systems.

5. SEGREGATION OF DUTIES

5.1 AUArts shall enforce segregation of duties to prevent conflicts of interest and reduce risk.
5.2 No individual, even if they have the administrative privileges to do so, may both approve the request and create, modify or delete any user access.

6. COMPENSATING CONTROLS

6.1 Where standard controls cannot be implemented, compensating controls must be documented, approved by IT Security, and provide equivalent risk mitigation. These controls shall be reviewed annually.

7. REVIEWING AND MONITORING

7.1 User access audits shall be conducted by Information Asset Owners for their in-scope Information Assets every 12 months at a minimum, with frequency of review increasing for higher risk processes and systems to ensure that current access privileges are relevant and appropriate.
7.2 Privileged accounts must be monitored and reviewed quarterly.

D. DEFINITIONS

Authorized Users: Students, staff, faculty, employees, and third-party users such as contractors, consultants, temporary users, suppliers, and service providers that access or manage organizational IT resources.

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.

E. RELATED POLICIES

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

F. RELATED LEGISLATION

- Alberta Protection of Privacy Act (POPA)
- Alberta Access to Information Act (ATIA)

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	All	Director, CTS	Vice President, Administration
01/16/2026	Content revisions	All	Manager, IT Security	Vice President, Finance and Operations