MOBILE DEVICE ACCEPTABLE USE POLICY

Policy Type:	Institutional	**Initially Approved:**	January 12, 2021
Policy Sponsor:	Vice President Administration	**Last Revised:**	
Primary Contact:	Facilities	**Review Scheduled:**	January 2026
Approver:	President and CEO		

A. PURPOSE

The purpose of this document is to define accepted practices, and responsibilities for the use of mobile devices authorized to access, store or manipulate AUArts information.

At the core of this policy is the concept that eligible employees agree to AUArts practices and technical controls in exchange for access to corporate resources (such as the network and email) through that device. It is important that the consequences and obligations of this arrangement are well-understood by the user.

It is the practice of AUArts to protect and maintain user safety, security and privacy while simultaneously protecting University information assets while using these tools.

Use of Mobile Devices owned and supplied by AUArts shall be primarily used for University business purposes, although reasonable personal use is acceptable.

B. SCOPE

This policy applies to all individuals connecting to AUArts information assets, including University data, systems, and applications while using Mobile Devices. Mobile Device means an electronic computing device such as a smartphone or tablet that provides access to AUArts systems or data from various locations including outside the University's physical location. This can be either an AUArts-owned device ("University-issued") or a personally owned device ("own-use"), and collectively referred to as "Mobile Device(s)".

C. POLICY STATEMENT

1. USER RESPONSBILITIES

1.1 University-issued devices remain the property of AUArts.
1.2 Where a Mobile Device is being used for University Business, the user assumes full responsibility for the physical security of the device and the information contained on the device.

1.3 Prior to accessing AUArts information from a Mobile Device, the user shall review and understand the responsibilities outlined in this policy.

1.4 Users can not expense or purchase with AUArts resources additional carrier services (e.g. roaming, increased data plan) without prior supervisor review and approval.

1.5 AUArts expects the user to assume certain responsibilities for any Mobile Device that contains University Information or connects to University resources. Specifically, users must ensure they:

a. maintain the device with the latest OS version and security patches
b. comply with all sections of the Acceptable Use Policy
c. agree to take responsibility for the security of their Mobile Devices and any AUArts information housed on the device
d. understand AUArts is not responsible for personal data that is lost or corrupt
e. understand protecting University data is a shared responsibility
f. report any suspected privacy or information breaches to the FOIP Coordinator

2. AUARTS RESPONSBILITIES

2.1 AUArts reserves the right to monitor security settings on any Mobile Devices connecting to the University network to ensure minimum security levels are maintained.

2.2 Monitoring for settings as a condition for connecting to the University network does not entail AUArts accessing the user's personal or other, non-work-related data on personally owned devices.

2.3 If a device fails to satisfy the minimum-security levels, it may be blocked from access until it meets the minimum requirements.

3. LOSS OR THEFT

3.1 If a Mobile Device is lost, stolen or suspected to be compromised in any way, the user must:

a. Notify their supervisor and the Helpdesk in the event a **University-issued** Mobile Device is lost or stolen.
b. Notify the Helpdesk in the event an **own-use** Mobile Device connecting to University systems or data is lost or stolen, so the device can be blocked from further access.
c. AUArts C&TS will remotely block access to the environment for lost or stolen Mobile Devices.
d. AUArts is not responsible for replacing or reimbursing users for own-use Mobile Devices.

4. APPLICATION AND DOWNLOADS

4.1 Users must take all reasonable steps to protect against the installation of unlicensed or malicious applications (malware).

4.2 For University-issued devices:

a. Downloading applications from a public application store (e.g. Apple's iTunes, Android's Play Store) for Personal Use is acceptable if the application complies with the AUArts Acceptable Use Policy.
b. Downloaded software must have a valid license for each prospective user and must not be pirated or shared in a way that contravenes the End-User-Licensing-Agreements (EULA).

5. BACKUPS AND FILE SHARES

5.1 The objective of backup/restore and file share access practices on Mobile Devices is to ensure University Information is appropriately protected from loss. Users must make every reasonable effort to ensure that personal information and AUArts information remain separate, specifically:
a. The user's personal or other, non-work-related data on own-use Mobile Devices is the sole responsibility of the user; AUArts is not responsible for loss, theft, or corruption of such data.
b. The user's personal or other, non-work-related data on Mobile Devices (e.g. personal photos, videos, music, etc.) should be moved/backed up to a personal computer or data source.
c. University Information protection is a shared responsibility between the user and the University.
d. University Information on Mobile Devices (e.g. documents, spreadsheets, emails) must be saved and backed up to an approved and managed AUArts storage location.
e. University Information must not be copied or backed up to an unapproved "cloud" or online storage service such as Drop Box, iCloud, Google Drive, etc.

6. FEATURES AND FUNCTIONS

6.1 Users accept that when connecting a Mobile Device to University resources, AUArts' security policy may be enforced on the device, which can include requirements such as a passcode, a passcode timeout, passcode complexity and encryption.
6.2 Users may be required to allow the installation of a mobile device management software agent on the user's Mobile Device before the Mobile Device can access an AUArts system.
6.3 The use of devices that are jail broken, "rooted" or have been subjected to any modification intended to bypass built-in protections are not permitted.
6.4 Users must take appropriate precautions to prevent others from obtaining access to University Information on their Mobile Device(s), as users will be responsible for all actions made with their AUArts credentials.
6.5 Users must not share individually AUArts-assigned passwords, PINs or other credentials.
6.6 Users are permitted to use any preferred email client (including Outlook) for personal communications, however, only the approved email service (Outlook) may be used for University related email communications.
6.7 Mobile Devices are not to be used to record meetings unless there is an authorized purpose for doing so, and documented notification to each of the meeting participants, according to collection rules in the FOIP Act.

7. PURCHASING

7.1 Unless previously approved, AUArts P-Cards must not be used to purchase applications for personal or University use without first checking with the Helpdesk regarding licensing agreements that may be in place.

7.2 Should approval to use an AUArts P-Card be issued for the purchase of an application, auto-renewals and in-app purchases should be disabled to prevent inadvertent charges from being made.

7.3 For security reasons, AUArts P-Card information should not be saved/stored in an app store account.

8. SAFETY

8.1 AUArts prohibits the use of Mobile Devices while driving a personal or rental vehicle on University business as it presents a hazard to the driver and the general public.

8.2 Use of Mobile Devices while stopped and legally parked in a safe location is acceptable.

9. DATA SECURITY AND PRIVACY OBLIGATIONS

9.1 All users shall abide by AUArts Information Security and Acceptable Use policies and practices when using Mobile Devices for University Business.

9.2 When using Mobile Devices for University Business, users must:

a. ensure the Mobile Device is physically secured from unintended access to University Information by following password, passcode, and encryption settings; and

b. take appropriate precautions to prevent others from obtaining access to University Information stored on Mobile Devices.

9.3 Most Mobile Devices provide location services. AUArts may only use location information that may be obtained as part of the normal management of the device for the sole purpose of locating the device if lost or stolen (with permission of the user), where a legitimate business requirement has been identified, or when assisting a user in distress or a user who is believed to be in distress. The University's use of location services is not permitted for tracking or monitoring individuals.

10. END OF EMPLOYMENT OBLIGATIONS

10.1 Availability of and access to AUArts networks and systems via a Mobile Device is subject to conditions of employment and/or contract terms, and shall be revoked upon end of employment.

10.2 Users must return all AUArts-owned Mobile Devices to the University at the end of employment, having reset the device to original factory settings so that the device is not locked or connected to a user account of any kind (e.g. Apple ID).

10.3 Users no longer employed at AUArts must permanently delete all University information stored on their owned-use device immediately upon end of employment.

11. e-DISCOVERY

11.1 In the event AUArts requires access to an AUArts-owned Mobile Device for e-discovery or internal investigation purposes, the user is obliged to immediately surrender the Mobile Device along with the necessary passcodes.

11.2 In the event AUArts requires access to an owned-use Mobile Device for e-discovery or internal investigation purposes, the user may be asked to grant access to the Mobile Device along with the necessary passcodes, but is not obliged to do so.

12. NON-COMPLIANCE

12.1 Violations of this policy may result in disciplinary action up to and including termination of employment.

12.2 In cases where local or international laws have been violated, AUArts has a responsibility to involve appropriate law enforcement agencies.

D. DEFINITIONS

FOIP means the Alberta *Freedom of Information and Protection of Privacy Act*

Mobile Device means an electronic computing device such as a smartphone or tablet that provides access to AUArts systems or data from various locations including outside the University's physical location. This can be either an AUArts-owned device ("University-issued") or a personally owned device ("own-use"), and collectively referred to as "Mobile Device(s)".

Mobile applications means software designed for any Mobile Device defined in this document.

User's Personal or Other Information means any information housed on the Mobile Device that is not included in the definition of Personal information under the FOIP Act; or any information housed on the Mobile Device that is not considered Work Product under the FOIP Act; or as University Information in this policy.

University Information means any information housed on the Mobile Device that is in the definition of Personal information under the FOIP Act; or any information defined as Work Product under the FOIP Act.

User means the employee who owns the device or to whom a University Mobile Device has been issued under this policy.

Public Information means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public according to the rules in the FOIP Act and AUArts policy.

Personal Use means use of a Mobile Device for non-University Business.

E. RELATED POLICIES

- Acceptable Use Policy
- Access to Information and Protection of Privacy Policy
- Code of Conduct Policy
- Information Security Policy
- Risk Management Policy

F. RELATED LEGISLATION

- Alberta *Freedom of Information and Protection of Privacy Act*

G. RELATED DOCUMENTS

- AUArts Mobile Device Guidelines

H. REVISION HISTORY

Date (mm/dd/yyyy)	Description of Change	Sections	Person who Entered Revision (Position Title)	Person who Authorized Revision (Position Title)