INFORMATION TECHNOLOGY: ACCEPTABLE USE POLICY

Policy Type:	Institutional	**Initially Approved:**	April 24, 2018
Policy 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. INTENT

This policy establishes the principles and controls governing the appropriate use of AUArts' information assets to ensure confidentiality, integrity, and availability in alignment with cybersecurity best practices and regulatory requirements.

B. SCOPE

This policy applies to all authorized users of AUArts information assets, regardless of location, device, or method of access, or hosting environment.

C. POLICY STATEMENT

1. ASSET PROVISION AND USE

1.1 AUArts will provide equipment and information assets necessary for the satisfactory completion of the duties and responsibilities of authorized users.
1.2 AUArts' Information Assets shall only be used for authorized activities and purposes related to Authorized Users' legitimate functions and in an appropriate manner.
1.3 Use and access to AUArts' Information Assets is permitted:
  a) When registered in a program of study
  b) When employed
  c) When fulfilling a contract, or
  d) As an authorized guest user

2. AUTHORIZED USER ACKNOWLEDGEMENT

2.1 Acceptance of this policy and related policies and procedures is a condition of employment, enrolment, or engagement
2.2 Users must acknowledge this policy upon onboarding and annually thereafter
2.3 Exceptions to this policy must be formally requested and approved by IT Security. All exceptions must be documented and time bound.

3. ACCESS CONTROL

3.1 Access shall be granted based on the principle of 'least privilege' and role-based access controls
3.2 Access rights shall be reviewed regularly and revoked immediately upon termination or role change
3.3 Multi-factor authentication is mandatory for all access to Information Assets
3.4 Passwords must meet complexity requirements
3.5 Sessions shall automatically timeout after 15 minutes of inactivity

4. CONDITIONS OF USE

4.1 All provided equipment remains the property of AUArts and may be inspected or recalled at any time without notice
4.2 Unauthorized use of Information Assets and equipment is prohibited, as it may increase AUArts' risk of exposure to loss, malicious software and cyberattack, network disruptions, service interruptions, and legal or regulatory compliance issues
4.3 Users should not expect privacy when using AUArts' Information Assets. AUArts may monitor, access, review, or disclose system activity where required to maintain IT operations, investigate security events, comply with legal obligations, or support authorized workplace investigations.
4.4 Personal devices accessing AUArts' networks must comply with mobile device management (MDM) and endpoint protection standards
4.5 Personal phones, tablets and laptops are allowed guest Wi-Fi access. Devices infected with malware will be disconnected immediately upon detection.

5. ACCEPTABLE USE

5.1 Users shall:
a) Comply with all AUArts' policies, procedures and guidelines regarding the use of AUArts Information Assets
b) Be aware that the files created on AUArts' Information Assets remain the property of AUArts and that the Intellectual Property of the data is subject to all AUArts' policies, procedures and guidelines
c) Store University data only in approved locations where it can be protected and backed up as part of AUArts' regular backup and recovery processes
d) Use Information Assets only for their intended and authorized purposes.
e) Information Technology resources must be used and managed in a responsible manner.
f) Limited personal use of AUArts Information Assets is permitted provided that such use:
i. Complies with this and all other AUArts policies;
ii. Does not interfere with the User's job performance or responsibilities;
iii. Does not compromise AUArts' organizational objectives
iv. Does not increase costs or consume excessive resources
v. Does not expose AUArts to legal, security, or reputational risk; and
vi. Does not impact the work of other users or AUArts operations.
g) Respect intellectual property rights and data ownership

h) Promptly report suspected or actual misuse of Information Assets, security incidents, data breaches, or policy violations to IT Services, Human Resources, or the User's manager, as appropriate
i) Return all AUArts Information Assets no later than the User's final day of employment or engagement, or upon request. AUArts reserves the right to recover costs associated with lost, damaged or unreturned assets, subject to applicable agreements.

5.2 Professional electronic communications

a) Electronic communications conducted using AUArts' Information Assets must be professional and consistent with AUArts' policies. University email accounts must not be used in a manner that implies institutional endorsement of personal viewpoints.
b) All forms of electronic communication are expected to reflect high ethical standards, mutual respect, and civility. Users must refrain from transmitting to others inappropriate images, sounds, or messages that might reasonably be considered harassing, fraudulent, threatening, obscene, defamatory, or otherwise violate applicable law or University policy.

6. PROHIBITED USE

6.1 Users shall not use AUArts' Information Assets to:

a) Create a negative impact on AUArts
b) Violate any laws, participate in a crime, commit fraud, or conduct unlawful activities including copyright infringement
c) Disruptive, fraudulent, harassing, threatening, obscene (including but not limited to racist, profane, and pornographic in nature), or malicious purposes is strictly prohibited.
d) Cause harm or disruption to AUArts' Information Assets
e) Alter or modify any operating system, software, hardware, or system configurations that compromise security or safety
f) Initiate actions that defeat or circumvent AUArts' security measures and restrictions
g) Conduct unauthorized network monitoring
h) Introduce malware harmful to the operation of any Information System
i) Install or distribute unauthorized or unlicensed software
j) Gain unauthorized access to systems
k) Interfere with, or disable, another user's access or systems operations
l) Share passwords or allow account use by others
m) Actively engage in procuring or transmitting material that violates sexual harassment or workplace laws and policies
n) Violate AUArts' policies, procedures, or
o) Access, copy or share Confidential, Internal Use, or Restricted data without authorization
p) Connect unauthorized networking devices (e.g., routers, switches, access points) to AUArts' networks.
q) Access or attempt to access network configuration settings without authorization
r) Engage in activities that intentionally consume excessive bandwidth or disrupt network performance

s) Alter or disable AUArts' security controls, endpoint protection tools, or monitoring systems.
t) Use information technology resources for commercial purposes unless authorized by the appropriate Dean or Director.

7. MONITORING AND LOGGING

7.1 Information Systems must have monitoring tools in place to detect and alert on unauthorized usage and anomalous behavior
7.2 Monitoring may occur:
  a) during normal IT operations, maintenance, or troubleshooting
  b) during investigations of suspected policy violations or cybersecurity incidents
  c) when required for legal, regulatory, or law-enforcement purposes
  d) to support workplace investigations authorized by AUArts' leadership
7.3 Logs shall be retained for at least 12 months and reviewed regularly
7.4 Alerts shall be configured for privilege escalation, data exfiltration, and policy violations
7.5 Monitoring systems shall integrate with a centralized SIEM platform

8. INCIDENT RESPONSE

8.1 Violations will trigger the Incident Response Plan coordinated by IT Security
8.2 Incidents shall be classified by severity and escalated per defined procedures
8.3 All incidents must be reported within 24 hours of detection
8.4 Post-incident reviews will be conducted to improve future response and recovery

9. RECOVERY AND CONTINUITY

9.1 Backup and recovery procedures shall be documented and tested annually
9.2 Business continuity plans shall include provisions for access restoration and data integrity

10. ENFORCEMENT

10.1 Policy violations may result in corrective actions, including suspension or termination of access
10.2 Evidence of noncompliance will be retained to support enforcement actions
10.3 Users may be subject to discipline or sanctions, up to and including termination, in accordance with collective agreements and/or other applicable University policies if non-compliance constitutes misconduct

D. POLICY REVIEW

1. This policy will be reviewed annually to ensure alignment with current security requirements and operational needs.

E. ROLES AND RESPONSIBILITIES

1. AUTHORIZED USERS

1.1 Understand and comply with this Policy and related documents
1.2 Complete all mandatory training and awareness programs related to information security, privacy, and acceptable use (e.g. cybersecurity awareness training), as required by AUArts, and applying that training in the use of Information Assets.

2. INFORMATION TECHNOLOGY

2.1 Maintain a current information asset inventory list
2.2 Maintain current records of all authorized users, including account information, and access privileges
2.3 Grant, modify, and revoke access privileges based on the principle of least privilege and documented business requirements.
2.4 Monitor network performance, traffic flow and resource utilization in support of operational reliability and security.
2.5 Support delivery, tracking and technical enablement of required security and acceptable use training, as applicable.

3. IT SECURITY

3.1 Promote and ensure compliance with this Policy and related security standards.
3.2 Investigate suspected or confirmed policy violations, security incidents, and misuse of Information Assets.
3.3 Lead policy review, security awareness initiatives, and incident response coordination in collaboration with Information Technology, Human Resources, and other stakeholders.

F. DEFINITIONS

Acceptable Use:	University information technology resources are to be used solely for activities related to the mission of the university, including, but not limited to teaching, learning, research and administration.
Authorized Users:	Students, staff, faculty, employees and third-party users such as contractors, consultants, temporary or guest 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.

G. RELATED POLICIES AND PROCEDURES

- Code of Conduct Policy
- Respectful Workplace Policy
- Student Conduct Policy
- Copyright Policy
- Access to Information and Protection of Privacy Policy
- IT User Access Policy
- Social Media Procedure
- Website Procedure

H. 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 review and minor revisions	All	Manager, IT Security	Vice President, Finance and Operations