INFORMATION TECHNOLOGY: INFORMATION CLASSIFICATION PROCEDURE

Procedure Type:	Institutional	**Initially Approved:**	May 2, 2011
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. INTENT

This procedure defines the basic classification levels applied to AUArts' Information Assets. These levels are applied after considering the applicability of the Alberta Protection of Privacy Act (POPA) to the individual information asset components. This document specifies the level of protection assigned to an information asset based on its assigned classification.

B. SCOPE

The Information Classification Procedure applies to all Information Assets at AUArts including those that are processed or managed by outside organizations on behalf of AUArts.

C. PROCEDURES

1. INFORMATION CLASSIFICATION:

1.1 AUArts shall use one of four classification designations to categorize individual Information Assets.

1.2 All electronic information shall be classified as described in the information asset classification scheme below.

1.3 The level of data protection required is based on the classification and value of the data being secured.

1.4 Under the provincial POPA legislation, all documents are subject to disclosure unless they are specifically excluded to protect the privacy of an individual or the confidential commercial data of suppliers.

1.5 At AUArts, privacy extends to identifiable personal information of faculty, staff and students, and privileged, commercial, competitive information often supplied to AUArts by suppliers or contractors.

1.6 When electronic copies of Confidential or Restricted information are taken off site, they shall be encrypted.

1.7 If there is any ambiguity with respect to Confidentiality, the information will be classified as Confidential until it can be definitively classified at a lower level.

2. INFORMATION ASSET CLASSIFICATION SCHEME

2.1 The classifications are:

Classification	Definition	Examples
Level 1: Public	• Information that is in the Public Domain and is intended for internal or external distribution, with no restrictions. • Public disclosure is its intended purpose for the benefit of AUArts.	• information posted to the AUArts' website • public announcements • annual reports • recruiting pamphlets • telephone directories including names of employees and business contact information.
Level 2: Internal Use	• Information not approved for general circulation outside the University • Information the disclosure or loss of which would inconvenience the University although it would unlikely result in financial loss or reputational damage	• internal memos sent to all members of a department • minutes of department meetings that are circulated to all members of a department • unpublished research data • anonymized or de-identified human subject data • electronic mail messages • operational procedures, plans and designs • budgets and accounts

Level 3: Confidential	• Information that is available only to authorized persons
	• Information the disclosure or loss of which could seriously impede the University's operations
	• Information the disclosure or loss of which may:
	  ○ adversely affect the University's operation; or
	  ○ cause reputational damage; and
	  ○ obligate the University to report to the government or other regulating body and/or provide notice to affected individuals.
		• faculty/staff employment applications, personnel files, date of birth, health information and personal contact information
		• admission applications
		• student enrollment status
		• personal data
		• donor or prospective donor name and contact information
		• information commonly used to establish identity such as a driver's license or passport
		• contracts
		• intellectual property
		• authentication verifiers including:
		  ○ passwords
		  ○ shared secrets
		  ○ cryptographic private keys

Classification	Definition	Examples

Level 4: Restricted	• Information that is:
	  ○ confidential; and
	  ○ subject to specific privacy and security safeguards under law, policy or contractual agreement.
	• Information the loss or disclosure of which could cause severe harm to individuals or the University
	• Information the loss or disclosure of which may obligate the University to report to the government or other regulating body and/or provide notice to affected individuals
		• payment card information including:
		  ○ PAN
		  ○ cardholder name
		  ○ CVV2/CVC2/CID
		• health information when it can be linked to an identifiable individual including:
		  ○ information about health status
		  ○ diagnostic, treatment or care information
		  ○ payment for health care
		• personal information of individuals located in the European Union (EU) as governed by the EU General Data Protection Regulation 2016/679 (GDPR), or personal information of other individuals governed by analogous international privacy legislation
		• information that is subject to special government requirements in the interests of national security

D. ROLES AND RESPONSIBILITIES

1. AUTHORIZED USERS:

1.1 Shall be responsible for recognizing personal data in their workflow that requires secure handling and taking reasonable precautions to prevent disclosure of the data.

2. INFORMATION ASSET OWNER:

2.1 Shall be responsible for classifying their Information Assets.
2.2 Shall review and update their asset classification and risk assessment annually. Attestation to the review is recorded in the IT Asset Inventory.
2.3 Shall review and update the Record Retention Schedule annually under the IT Backup, Recovery and Disposal Procedure.

3. INFORMATION TECHNOLOGY (IT):

3.1 Is responsible for ensuring appropriate information classification procedures are established and that compliance is maintained.
3.2 Will maintain a list of Information Assets and review the information asset classification annually to evaluate its effectiveness.
3.3 Shall adopt control and distribute encryption tools and software to enable users with approved business requirements to transport data classified as Confidential or Restricted off campus for approved business purposes.

4. IT SECURITY

4.1 Shall monitor external handling of AUArts' data resources to ensure that protection consistent with the data classification is being enforced.

a) If monitoring exposes any unexpected risk of exposure to Protected AUArts' data resources, an investigation will be undertaken to prevent disclosure.
b) Corrective action shall be undertaken to protect the exposed AUArts' Information Assets.
c) If needed, procedures may be reviewed and an update recommended where a coverage gap is discovered within any documented process.

E. 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 individual responsible for the management of an information asset.

F. RELATED POLICIES

- Information Security Policy
- IT Backup, Recovery and Disposal Procedure

G. RELATED LEGISLATION

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

H. RELATED DOCUMENTS

- Information Asset Inventory
- Record Retention Schedule
- IT - Classified Data Identification and Protection - Compliance Guideline

I. 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	Review and content updates	Legislation references from FOIP to POPA and ATIA	Manager, IT Security	Vice President, Finance and Operations