IT: INFORMATION CLASSIFICATION PROCEDURE

Procedure Type:	Institution	**Initially Approved:**	May 2, 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 procedure defines the basic classification levels applied to AUArts information assets. These levels are applied after considering the applicability of the Freedom of Information and Protection of Privacy (FOIP) act 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 three classification designations to categorize individual information assets. The level of data protection required is based on the classification and value of the data being secured. Under the provincial FOIP 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. In the case of AUArts, privacy extends to faculty, staff and students' identifiable personal information and privileged, commercial, competitive information often supplied to AUArts by suppliers or contractors. The classifications are:

Classification	Definition
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. Examples include annual reports, recruiting pamphlets, information posted to the AUArts website, and telephone directories.
Internal Use - Not Protected	Information that is not intended for use outside of the College but could be requested under a FOIP request. All internal documents not specifically authored for public consumption or communicating FOIP protected personal information are included. Where misinterpretation of, for example, an unapproved proposal could be damaging to the public image, reputation, or credibility of the college, the document should be conspicuously labeled Draft, Unapproved, For Discussion or the like to prevent misunderstanding. Examples would include most electronic mail messages, operational procedures, plans and designs, budgets and accounts, and some categories of aggregate student information.
Internal Use-Protected	Information that is available only to authorized employees. Loss or disclosure of Protected information would constitute a breach of the privacy protection provisions of FOIP legislation. This information includes specific categories of student information, employee records and proprietary, competitive, commercial information received from suppliers. Protected information should not be copied or removed from the secure storage without specific authority.

1.2 All electronic information shall be classified as described in the above information asset classification scheme. The classification of an information asset component shall dictate the level of protection it receives.

1.3 When electronic copies of Internal Use - Protected information are taken off site, they shall be encrypted.

Roles and Responsibilities

2. Authorized Users:

2.1 Shall be responsible for recognizing personal data in their workflow that requires secure handling and taking reasonable precautions to prevent disclosure of the data. Personal data is always classified Internal Use – Protected.

3. Information Asset Owner:

3.1 Shall be responsible for classifying their information assets. Information Asset owners shall review and update their asset classification and risk assessment annually. Attestation to the review is recorded in the IT Asset Inventory.

4. Manager, Software Services:

4.1 Will maintain a list of Information Assets and review the information asset classification annually to evaluate its effectiveness. The Information Asset list shall also contain the Record Retention Schedule prepared by the information asset owner under the Backup, Recovery and Disposal Procedure.

5. Computing and Technical Services (C+TS):

5.1 Is responsible for ensuring appropriate information classification procedures are established and that compliance is maintained.

5.2 Shall adopt control and distribute encryption tools and software to enable users with approved business requirements to transport Internal Use – Protected data off campus.

5.3 Shall monitor external handling of AUArts data resources to ensure that protection consistent with the data classification is being enforced. If monitoring exposes any unexpected risk of exposure to Protected AUArts data resources, an investigation will be undertaken to prevent disclosure. Corrective action shall be undertaken to protect the exposed AUArts information assets. If needed, procedures may be reviewed and an update recommended where a coverage gap is discovered within any documented process.

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 individual responsible for the management of an information asset.

E. RELATED POLICIES

- AUArts Information Security Policy

F. RELATED LEGISLATION

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

G. RELATED DOCUMENTS

- Information Asset Inventory
- IT - Classified data identification and protection - Compliance Guideline

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		Director, CTS	