Canadian Access Federation: Trust Assertion Document (TAD)

Purpose

A fundamental requirement of Participants in the Canadian Access Federation is that they assert authoritative and accurate identity attributes to resources being accessed, and that Participants receiving an attribute assertion protect it and respect privacy constraints placed on it by the asserting Participant.

To accomplish this practice, CANARIE requires Participants to make available to all other Participants answers to the questions below.

Canadian Access Federation Requirement

Currently, the community of trust is based on “best effort” and transparency of practice. Each Participant documents, for other Participants, their identity and access management practices, which they can confidently meet. Each Participant should make available to other Participants basic information about their identity management system and resource access management systems registered for use within the Canadian Access Federation. The information would include how supported identity attributes are defined and how attributes are consumed by services.

Publication

Your responses to these questions must be:

1. submitted to CANARIE to be posted on the CANARIE website; and
2. posted in a readily accessible place on your web site.

You must maintain an up-to-date Trust Assertion Document.

Canadian Access Federation: Trust Assertion Document (TAD)

1. Canadian Access Federation Participant Information

1.1.1. Organization name: Cambrian College of Applied Arts and Technology

1.1.2. Information below is accurate as of this date: April 25, 2016

1.2 Identity Management and/or Privacy information

1.2.1. Where can other Canadian Access Federation Participants find additional information about your identity management practices and/or privacy policy regarding personal information?

By contacting the individual below.

1.3 Contact information

1.3.1. Please list person(s) or office who can answer questions about the Participant's identity management system or resource access management policy or practice.

Name: Aamir Iqbal

Title or role: Manager, Infrastructure Support Services / IT Security Officer

Email address: aamir.iqbal@cambriancollege.ca

Telephone: (705) 566-8101 x6271

2. Identity Provider Information

Two criteria for trustworthy attribute assertions by Identity Providers are: (1) that the identity management system be accountable to the organization's executive or business management, and (2) the system for issuing end-user credentials (e.g., userids/passwords, authentication tokes, etc.) has in place appropriate risk management measures (e.g. security practices, change management controls, audit trails, accountability, etc.).

2.1 Community

2.1.1. As an Identity Provider, how do you define the set of people who are eligible to receive an electronic identity? If exceptions to this definition are allowed, who must approve such an exception?

By employment/enrolment status, e.g., FT, PT. Different rules apply to contractors and guest accounts. Exceptions are approved by the hiring/responsible manager and are vetted by the IT Security Officer.

2.1.2. What subset of persons registered in your identity management system would you identify as a "Participant" in SAML identity assertions to **CAF** Service Providers?

All staff, faculty, and students.

2.2 Electronic Identity Credentials

2.2.1. Please describe, in general terms, the administrative process used to establish an electronic identity that results in a record for that person being created in your electronic identity database? Please identify the office(s) of record for this purpose.

All identities are processed through the Registrar's office for students and Human Resources for staff/faculty. Once students are registered and staff/faculty have a hiring recommendation form processed, their accounts are automatically created through various system processes.

2.2.2. What authentication technologies are used for your electronic identity credentials (e.g., Kerberos, userID/password, PKI, ...) that are relevant to Canadian Access Federation activities? If more than one type of electronic credential is issued, how is it determined who receives which type? If multiple credentials are linked, how is this managed (e.g., anyone with a Kerberos credential also can acquire a PKI token) and audited?

UserID/password.

2.2.3. If your electronic identity credentials require the use of a secret password or PIN, and there are circumstances in which that secret would be transmitted across a network without being protected by encryption (e.g., "clear text passwords" are used when accessing campus services), please identify who in your organization can discuss with any other Participant concerns that this might raise for them:

N/A

2.2.4. If you support a "single sign-on" (SSO) or similar campus-wide system to allow a single user authentication action to serve multiple applications, and you will make use of this to authenticate people for **CAF** Service Providers, please describe the key security aspects of your SSO system including whether session timeouts are enforced by the system, whether user-initiated session termination is supported, and how use with "public access sites" is protected.

N/A

2.2.5. Are your primary electronic identifiers for people, such as "NetID," eduPersonPrincipalName, or eduPersonTargetedID considered to be unique for all time to the individual to whom they are assigned? If not, what is your policy for re-assignment and what is the interval between such reuse?

Primary electronic identifiers are considered unique for all time.

2.3 Electronic Identity Database

2.3.1. How is information in your electronic identity database acquired and updated? Are specific offices designated by your administration to perform this function? Are individuals allowed to update their own information on-line?

Initial electronic ID information is acquired during student registration or during the hiring of hiringstaff/faculty. Updates to information (other than passwords) are handled through the Registrar's office or by Human Resources.

2.3.2. What information in this database is considered "public information" and would be provided to any interested party?

First name, last name, work telephone number, and work email address.

2.4 Uses of Your Electronic Identity Credential System

2.4.1. Please identify typical classes of applications for which your electronic identity credentials are used within your own organization.

Access to the network, storage (file shares), corporate and academic applications, email, learning management system, VPN access, portals.

2.5 Attribute Assertions

Attributes are the information data elements in an attribute assertion you might make to another Canadian Access Federation Participant concerning the identity of a person in your identity management system.

2.5.1. Please describe the reliability of your identity provider attribute assertions?

Enrolment Services and Human Resources confirm student and employee details respectively. Visitor/Guest information is confirmed by the sponsor.

2.5.2. Would you consider your attribute assertions to be reliable enough to:

a) control access to on-line information databases licensed to your organization? **Yes**

b) be used to purchase goods or services for your organization? **No**

c) enable access to personal information such as student record information? **No**

2.6 Privacy Policy

Canadian Access Federation Participants must respect the legal and organizational privacy constraints on attribute information provided by other Participants and use it only for its intended purposes.

2.6.1. What restrictions do you place on the use of attribute information that you might provide to other Canadian Access Federation participants?

Use of attribute information is governed by the college's privacy policy.

2.6.2. What policies govern the use of attribute information that you might release to other Canadian Access Federation participants?

The privacy policy referenced below.

2.6.3. Please provide your privacy policy URL.

Internal privacy policy is attached to this document.

3. Service Provider Information

Service Providers, who receive attribute assertions from another Participant, shall respect the other Participant's policies, rules, and standards regarding the protection and use of that data. Such information must be used only for the purposes for which it was provided.

Service Providers are trusted to ask for only the information necessary to make an appropriate access control decision, and to not misuse information provided to them by Identity Providers. Service Providers must describe the basis on which access to resources is managed and their practices with respect to attribute information they receive from other Participants.

3.1 Attributes

3.1.1. What attribute information about an individual do you require in order to manage access to resources you make available to other Participants? Describe separately for each service application that you offer to CAF participants.

We would only use attribute information to support the eduroam service.

3.1.2. What use do you make of attribute information that you receive in addition to basic access control decisions?

None.

3.1.3. Do you use attributes to provide a persistent user experience across multiple sessions?

No.

3.1.4. Do you aggregate session access records or record specific information accessed based on attribute information.

No.

3.1.5. Do you make attribute information available to other services you provide or to partner organizations?

No.

3.2 Technical Controls

3.2.1. What human and technical controls are in place on access to and use of attribute information that might refer to only one specific person (i.e., personally identifiable information)? For example, is this information encrypted for storage in your system?

Access to information is restricted to authorized individuals only for the performance of their work. Stored information is not encrypted.

3.2.2. Describe the human and technical controls that are in place on the management of super-user and other privileged accounts that might have the authority to grant access to personally identifiable information?

Management of super user and other privileged accounts is restricted to the IT Security Officer and system administrators only.

3.2.3. If personally identifiable information is compromised, what actions do you take to notify potentially affected individuals?

Affected individuals are contacted directly by the IT Security Officer and/or the Privacy Officer.

4. Other Information

4.1 Technical Standards, Versions and Interoperability

4.1.1. Identify the SAML products you are using. If you are using the open source Internet2 Shibboleth products identify the release that you are using.

N/A

4.1.2. What operating systems are the implementations on?

N/A

4.1.3. What versions of the SAML protocol (1.1 or 2.0) do you support in your implementations?

N/A

4.2 Other Considerations

4.2.1. Are there any other considerations or information that you wish to make known to other Canadian Access Federation Participants with whom you might interoperate? For example, are there concerns about the use of clear text passwords or responsibilities in case of a security breach involving identity information you may have provided?

None.

Cambrian College of Applied Arts and Technology	No. *E06*	Pages *1 of 9*
	Approved by: **Executive Committee**	
Title: Cambrian College Internal Privacy Policy	**Effective Date** **December 2006**	**Replaces the Freedom of Information and Protection of Privacy Act Procedures and Policy (1988)**

Overview

Cambrian College is subject to the requirements of *Freedom of Information and Protection of Privacy Act* ("FIPPA"). In summary, FIPPA has two purposes.

i) It gives individuals access to recorded information held by the College.

ii) It regulates "personal" information in the possession of the College.

The following policy describes the obligations of the college and its staff under the Act. At the end of the policy are summarized the rules and expectations. Staff members are expected to review and comply with this policy. A failure to do so will be considered a serious employment matter and may give rise to legal liability.

Access Rights – General

FIPPA allows individuals access to recorded information in the custody or control of the College. For the general purposes of staff you should be aware of the following:

i) the access right only applies to recorded information;

ii) the information must be in the custody of or under the control of the College;

iii) not all information is subject to access requests – FIPPA contains a number of exemptions which will authorize (and in some cases require) the College to deny access to information;

iv) access requests must be in writing and must be accompanied by a payment to the College of $5 to be valid; and

v) access requests must normally be responded to within thirty (30) days.

Because the College is under strict time limits, staff members who receive such access requests must immediately forward the same to the College's FOI Coordinator, care of Human Resources, extension 7443. A failure to do so may have serious consequences for the College.
A second purpose for reporting access requests is that the College must report statistics on access requests annually to the Ontario Privacy Commissioner.

Regulation of Personal Information – Overview

FIPPA regulates personal information in the custody or control of the College. Specifically, it places restrictions on how the College collects, uses and discloses personal information. It also imposes rules on how long the College must keep personal information, and how it is to be kept secure.

What is "Personal Information"?

Personal information is information "about an identifiable individual". It includes but is not limited to the following:

- information on race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital or family status;
- information relating to medical, criminal, employment history or education or to the individual's financial transactions;
- identifying numbers and symbols;
- address, telephone number, fingerprints, blood type;
- personal views or opinions except as they relate to another individual;
- an individual's name where it appears with other personal information or where disclosure of the name would reveal personal information;
- views or opinions expressed about an individual; and correspondence that is sent to an institution by an individual where that correspondence is implicitly or explicitly of a confidential nature, as well as replies which would reveal the contents of the original letter.

When Can the College Collect Personal Information?

FIPPA deals with two types of collection:

- direct collection – from the affected person; and
- indirect collection – from a source other than the affected person.

The College can ONLY collect personal information (whether directly or indirectly) in one of the following three circumstances:

- where collection is expressly authorized by statute;
- where the information is used for the purposes of law enforcement;
- or where the information is necessary for the proper administration of a lawfully authorized activity.1

Direct Collection – Our Obligations

FIPPA imposes different rules depending on whether the information is collected directly from the individual or indirectly from another source. For direct collections, the College is required to notify affected individuals of the following:

- the legal authority for the collection;
- the principal purpose or purposes for which the information is intended to be used; and
- the title, business address and telephone number of the College official who can answer questions about the collection.

It should be noted that FIPPA does not require the College to obtain consent for the collection of personal information so long as the information is collected directly from individuals.

Indirect Collection – Our Obligations

FIPPA permits indirect collection of personal information only in limited circumstances. These include the following:

1 Normally, in determining whether an activity is "lawfully authorized", consideration should be given to the College's empowering statute. Currently, this is the *Ontario Colleges of Applied Arts and Technology Act, 2002* which states in part:

"The objects of the colleges are to offer a comprehensive program of career-oriented, post-secondary education and training to assist individuals in finding and keeping employment to meet the needs of employers and the changing work environment and to support the economic and social development of their local and diverse communities."

"In carrying out its objects, a college may undertake a range of education-related and training-related activities, including but not limited to,

a) entering into partnerships with business, industry and other educational institutions;
b) offering its courses in the French language, where the college is authorized to do so by regulation;
c) adult vocational education and training;
d) basic skills and literacy training;
e) apprenticeship in-school training; and
applied research."

- where consent to indirect collection is provided;
- where a disclosure to the College is otherwise permissible under the disclosure provisions of FIPPA (discussed under the heading 'When Can the College Disclose Personal Information?' below);
- where the Ontario Privacy Commissioner authorizes the collection;
- if the information is in a report from a report agency in accordance with the *Consumer Reporting Act;*
- if it is collected to determine suitability for an honour or award to recognize achievement or service;
- if it is collected for a proceeding or a possible proceeding before a court or tribunal;
- if it is collected for law enforcement purposes; or
- if another manner of collection is authorized under another statute.

Normally notice of the collection in the form described under the heading 'Direct Collection – Our Obligations' above must be given to the individual except under certain circumstances where access to the information can be denied under certain law enforcement sections of FIPPA (i.e., where the information is being collected for certain law enforcement proceedings or anticipated proceedings).

When Can the College Use Personal Information?

The College may only use personal information in its custody or control in limited circumstances. Normally the uses must be restricted to those for which the affected party has previously been given notice at the time of collection or for a "consistent purpose".
FIPPA defines a "consistent purpose" as one the requester might have reasonably expected. For example, if an individual is given notice that his or her address is being collected to send a magazine subscription it would likely be reasonably consistent to use the address to send a subscription renewal form.
Personal information may only be used for other purposes if one of the following exceptions applies:

- where the individual identifies the particular information and consents to its use; or
- for a purpose for which it may be disclosed under the disclosure provisions of the Act, (described under the heading 'When Can the College Disclose Personal Information?' below.)

In addition, under the June 2006 amendments to the Act, the College may use alumni records for the purposes of its own fundraising activities if the personal information is reasonably necessary for the fundraising activities and provided that certain steps are followed.[2]

When Can the College Disclose Personal Information?

Institutions may only disclose personal information in their custody or control under certain circumstances, including the following:

- where an access request is made and the Act permits granting of access;
- where the individual identifies the information and consents to its use;
- for the purpose for which it was collected or for a consistent purpose (i.e., one which the individual might have reasonably expected);
- for the purpose of complying with a federal or Ontario law or with a treaty, agreement or arrangement under such authority;
- where disclosure is to an institution or law enforcement agency in Canada to aid in an investigation with a view to a law enforcement proceeding or from which such a proceeding is likely to result;
- in compassionate circumstances to contact next of kin or a friend of an ill, injured or deceased person;
- to an MPP who has been authorized by the affected person to make inquiry on the person's behalf (or by the next of kin where the affected person is incapacitated);
- to a bargaining agent who has been authorized by the affected person to make inquiry on the person's behalf (or by the next of kin where the affected person is incapacitated);
- to the responsible Minister of the Ontario Government;
- to the Ontario Privacy Commissioner; or
- to the federal government to facilitate the auditing of a shared cost program.

Under the June 2006 amendments to FIPPA , the College may also disclose personal information

[2] These steps include the following: (a) giving notice to the contacted person, upon first contact, of his or her right to request that solicitation cease; (b) providing similar notices periodically thereafter when making additional solicitation approaches to the individual; and (c) periodically publishing a general notice of an individual's right to request that fundraising solicitation cease (e.g., through the College's web page or other printed publications). If asked to cease soliciting for fundraising, the College must stop approaching the individual.

for the purposes of fundraising activities (for example to its printing contractor or to a fundraising foundation) if the information is reasonably necessary for fundraising and the College enters an written agreement with the receiving party which meets certain requirements. These agreement requirements include the following:

- compliance with the requirement to give initial and periodic notice to individuals regarding their right to request that disclosure for fundraising cease;
- granting access to an individual's personal information held by the foundation or other recipient if requested by the individual; and
- ceasing the use of personal information for fundraising purposes if requested by the individual.

How Long Must the College Retain Personal Information?

Personal information must be retained for a period of at least one year from its use unless the affected individual consents to a shorter period. Personal information should not be destroyed prior to this time and may be subject to longer retention periods under the College's retention schedule.

Be aware that different departments within the College will have different retention policies and length of periods for which they retain information. If you have questions about how long a specific department will retain a document, please contact that department for clarification.

Security – General

Staff members are required to prevent unauthorized access to records and to define, document and put in place specific security measures. Each department is expected to do so. Security measures to be considered should include the following: computer use policies (e.g., password restrictions, shutting off computers while not in use etc.), firewalls, physical security (e.g., locking cabinets and offices) and administrative protocols (e.g., limiting staff access to certain files).

Security – Upon Disposal of Personal Information

When disposing of personal information the College is required to use "reasonable steps" to ensure information cannot be reconstructed or retrieved. A disposal record must be maintained identifying which information has been destroyed or transferred to the Archives of Ontario. In addition FIPPA requires that measures be taken to ensure security and confidentially during storage, transportation, handling and destruction. Specific measures are not outlined in the Act,

but any measures taken must consider the "nature of the personal information to be destroyed or transferred".

Accuracy

The College and its staff must take reasonable steps to ensure that personal information is not used unless it is accurate and up to date. In addition, individuals have the right to request correction to their own personal information if they believe an error or omission exists. If the correction is not made the requester may require that a statement of disagreement be attached reflecting that a correction was requested but not made. In addition, the requester may require that an institution notify any parties to whom the personal information was disclosed in the previous year of the correction or statement of disagreement.
Normally request for correction made under FIPPA must be responded to within thirty (30) days. Any such requests for correction should be immediately forwarded to the College's FOI Coordinator for review and advice.

Also, like access requests, the College must report correction requests annually to the Ontario Privacy Commissioner.

Personal Information Banks

Personal information banks are defined to include any collection of personal information that is organized and capable of being retrieved using an individual's name or some other identifier. This may include, for example, a student or alumnus record, or a record of potential donors to the College.

The Act requires the Minister to publish an annual index of personal information banks and to publish certain information associated with the banks, including how the information contained in the bank is regularly used or disclosed. FIPPA also requires institutions to attach or link to personal information banks a listing of any "non-regular" uses or disclosures of personal information contained in the banks. If information is used or disclosed for the purpose for which it was obtained or compiled, but that use or disclosure is not contained in the Minister's index, the institution must notify the Minister of the use or disclosure and ensure that is included in the index.
College staff members responsible for any personal information banks are requested to cooperate with College's FOI Coordinator to ensure steps are in place to comply with these obligations.

Records Not Covered by the Act

The above policy applies to recorded information covered by FIPPA. A limited number of documents are not subject to the Act. However, as a general matter, such documents should normally be treated in a fashion similar to that set out in FIPPA where reasonable.

Specifically FIPPA does not apply to the following:

A) Records "collected, prepared, maintained or used by or behalf of an institution" in relation to the following:

- proceedings or anticipated proceedings before a court, tribunal or other entity relating to labour relations or to the employment of a person by the institution;
- negotiations or anticipated negotiations relating to labour relations or to the employment of a person by the institution between the institution and a person, bargaining agent or party to a proceeding or an anticipated proceeding; and
- meetings, consultations, discussions or communications about labour relations or employment related matters in which the institution has an interest.

However, four subcategories of labour relations-related and employment-related documents are not included in this exemption, and are therefore subject to FIPPA. These are the following:

- agreements between institutions and trade unions;
- agreements between institutions and one or more employees ending proceedings before a court, tribunal or other entity relating to labour relations or employment;
- agreements between an institution and one or more employees relating to negotiations about employment related matters between the institution and employees; and
- employee business expense accounts submitted for reimbursement.

B) Since the June 2006 amendments to the Act, FIPPA does not apply to records "respecting or associated with research conducted or proposed by an employee of an educational institution or by a person associated with an educational institution."

However, information regarding the "subject matter" of research and "the amount of funding being received with respect to research" will still be subject to disclosure. Moreover, the Act will continue to apply to "evaluative or opinion material compiled in relation to research" for the purposes related to refusing disclosure.

C) Since the June 2006 amendments to FIPPA came into effect, the Act does not apply to records "of teaching materials collected, prepared or maintained by an employee of an educational institution or by a person associated with an educational institution for use at the educational institution."

However, the Act will continue to apply to "evaluative or opinion material compiled in relation to teaching materials" for the purposes related to refusing disclosure.

If you have any questions with respect to this Privacy Policy, please contact the College's Access and Officer, care of Human Resources, at extension 7443, or email at humanresources@cambrianc.on.ca