Canadian Access Federation:
Trust Assertion Document (TAD) for Service Providers

Purpose

Identity attributes are characteristics of an identity -- such as a name, department, location, login ID, employee number, e-mail address, etc.

A fundamental requirement of Participants in the Canadian Access Federation (CAF) is that by their authority they send accurate identity attributes to other Participants to allow access to resources, 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 in this document.

Canadian Access Federation Requirement

The CAF 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 makes 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 includes how supported identity attributes are defined and how attributes are consumed by services.

Publication

Your responses to these questions must be submitted to CANARIE to be posted on the CANARIE website. You must maintain an up-to-date Trust Assertion Document.

1. Participant Information

1.1 Organization Name: TrackPoint Technologies Inc.

1.2 Information below is accurate as of this date: 06/16/2026

1.3 Contact Information

1.3.1. Please list the office, role, department, or individual who can answer questions about the Participant's identity management system or resource access management policy or practice.

Note: This information should be for a department or office rather than an individual, in order to avoid responses going unanswered if personnel changes occur.

Department (or Contact Name): Technical Support Team, TrackPoint Technologies Inc.

Email Address: support@trackpoint.ai

Telephone: (639) 317-7531

1.4 Identity Management and/or Privacy Information

1.4.1. What policies govern the use of attribute information that you might release to other CAF Participants? If policies are available online, please provide the URL.

Use of identity attributes received through CAF is governed by TrackPoint's Terms of Service, Privacy Policy, and Acceptable Use Policy, together with TrackPoint's compliance with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Where a customer institution provides a Data Processing Agreement, the terms of that agreement also apply.

Terms of Service: https://www.trackpoint.ai/terms-conditions
Privacy Policy: https://www.trackpoint.ai/privacy-policy
Acceptable Use Policy: https://www.trackpoint.ai/usage-policy

1.4.2. Please provide your Privacy Policy URL, as well as information regarding any other policies that govern the use of attribute information that you might release to other CAF Participants.

Privacy Policy: https://www.trackpoint.ai/privacy-policy

TrackPoint complies with PIPEDA and stores all user data within Canada. Attributes received via SSO are used only to authenticate users and provision and maintain their accounts.

2. Identity Provider Information (FIM and/or eduroam)

Not applicable

3. Service Provider Information (Federated Identity Management and/or eduroam)

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? Describe each service that you offer to CAF Participants separately (one service per row).

Service Name	Is this an R&S service?	Attributes Required	Rationale	Is information shared with others?
eduroam	N/A	Not applicable. TrackPoint does not operate or participate in eduroam.	Not applicable	Not applicable
TrackPoint.ai **platform (SAML 2.0 SSO)**	☐	• **user identifier** (SAML NameID, e.g. eduPersonPrincipalName) • **person name** (givenName + sn) • **email address** • **affiliation** (eduPersonScopedAffiliation)	For authentication, account provisioning, and authorization. The identifier links the user to their TrackPoint account; name and email populate the account and send service notifications; affiliation is used to make access-control decisions such as role and licensing tier.	No

3.2 Technical Controls

Technical controls are a basis for controlling access to and usage of sensitive data and are expected to be applied across all services. If there are exceptions for a particular service(s), please describe these exceptions.

3.2.1. Describe the human and technical controls in place for access to and use of attributes considered personally identifiable information.

Identity attributes received through SSO are handled within Google Cloud Platform. Authentication is managed through Firebase Authentication, and any attribute data we retain is stored in Firestore. We run separate GCP projects and environments for development and production, so production data containing personally identifiable information is isolated from development and testing. Access to production data is limited to a small number of authorized personnel on a least-privilege basis. Data is encrypted in transit (TLS 1.3) and at rest (AES-256) and is stored in Canada. Attributes are used only to authenticate the user and to provision and maintain their TrackPoint account.

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

Infrastructure and technical accounts: Privileged access to our Google Cloud Platform environment is managed through GCP Identity and Access Management (IAM). Only a small number of named developers hold administrative roles, granted on a least-privilege basis, and production and development run in separate GCP projects so elevated access in one does not carry over to the other. Administrators sign in with their own individual accounts rather than shared logins, access is removed promptly when no longer required, and application secrets and credentials are held in a secured, access-controlled store and are never hardcoded in application code.

Application administrators within customer organizations: Customer organizations have administrator users in the TrackPoint platform who can manage their own users and view account and usage information for their organization only. These administrators have no access to the underlying infrastructure, databases, or other organizations' data, and their permissions are role-based and scoped to their own organization. Each customer manages its own administrators, and TrackPoint provisions or removes them at the customer's direction.

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

If a confirmed or suspected breach involves personal information, TrackPoint follows a documented incident-response process aligned with PIPEDA. We first contain the incident and assess its scope, including which individuals and which data elements are affected.
Where a breach creates a real risk of significant harm, we notify affected individuals as soon as feasible. The notice explains what happened, the personal information involved, what we are doing to reduce the harm, the steps individuals can take to protect themselves, and a contact for questions.
Because we receive identity attributes from partner institutions through CAF, we also promptly notify the affected institution (the asserting Participant) when its users or attribute data are involved, so it can coordinate a response on its side.
We retain records of all breaches and the remedial actions taken, whether or not notification is required, and we review each incident to prevent recurrence.

3.3 Other Considerations

3.3.1. Are there any other considerations or information that you wish to make known to other CAF Participants with whom you may interoperate?

TrackPoint participates in CAF solely as a Service Provider using SAML 2.0; we do not operate an Identity Provider or eduroam. We coordinate directly with each institution's identity team on SAML metadata exchange and attribute release.
We request only the minimum attributes needed to authenticate and provision a user: a unique identifier (SAML NameID, typically eduPersonPrincipalName), name, email, and eduPersonScopedAffiliation.
All user data is stored in Canada and is never used to train AI models.