Fédération canadienne d'accès :
Confirmation de fiabilité (DCF) pour les organisations participantes

But

Les attributs sont les « paramètres » d'une « identité » (nom, département, emplacement, identifiant, nombre d'employés, courriel, etc.).

Une exigence que doivent absolument respecter les organisations qui adhèrent à la Fédération canadienne d'accès (FCA) consiste à transmettre aux autres participants les attributs exacts des identités sans lesquels on ne pourra accéder aux ressources offertes. Parallèlement, les participants qui obtiennent les attributs dont la véracité a été confirmée sont tenus de les protéger et de respecter les contraintes qui s'y appliquent, fixées par l'organisation d'origine.

Dans cette optique, CANARIE demande à l'organisation de transmettre aux autres participants de la FCA les réponses aux questions qui suivent.

Exigence de la Fédération canadienne d'accès

La confiance qui règne au sein de la communauté de la FCA repose sur les « meilleurs efforts possibles » et la transparence des pratiques. Chaque organisation fournit aux autres participants la documentation sur ses pratiques en gestion des identités et des accès qu'elle sait pouvoir respecter. Elle met à leur disposition des renseignements de base sur les systèmes de gestion des identités et d'accès aux ressources qu'elle a inscrits à la FCA. Ces renseignements comprennent la manière dont les attributs identitaires sont définis et la façon dont les services utilisent ces attributs.

Publication

Les réponses aux questions qui suivent seront remises à CANARIE, qui les affichera sur son site Web. Il revient à l'organisation de garder à jour le Document de confirmation de fiabilité (DCF).

1. Renseignements sur le participant

1.1 Nom de l'organisation : Université Sainte-Anne

1.2 Les informations qui suivent étaient exactes le 06/28/2023

1.3 Coordonnées

1.3.1. Veuillez indiquer le bureau, le service, le département ou la personne en mesure de répondre aux questions sur le système de gestion des identités ou les politiques/pratiques concernant l'accès aux ressources de l'organisation.

Remarque : Il est préférable que ces renseignements se rapportent à un département ou à un bureau plutôt qu'à une personne pour qu'on puisse obtenir une réponse aux questions si jamais un changement survient au niveau du personnel.

Département (ou nom du contact) : André Roberge

Courriel : Andre.Roberge@usainteanne.ca

Téléphone : (902) 260-3027

1.4 Gestion des identités / Informations sur la protection des renseignements personnels

1.4.1. Quelles sont les politiques qui régissent l'usage des attributs que l'organisation pourrait transmettre aux autres participants de la FCA? Si ces politiques peuvent être consultées en ligne, veuillez en fournir l'URL.

En plus de notre propre politique sur la vie privée mentionnée ci-dessous, nous suivons les procédures décrites dans les lois fédérales et provinciales pertinentes.

1.4.2. Veuillez indiquer l'URL de votre politique concernant la protection des renseignements personnels et fournir des renseignements sur les autres politiques éventuelles régissant l'usage des attributs que l'organisation pourrait transmettre aux autres participants de la FCA.

https://www.usainteanne.ca/politique-sur-la-vie-privee

2. Renseignements sur le fournisseur d'identités (GFI / eduroam)

Le fournisseur d'identités doit respecter deux critères pour confirmer la fiabilité des attributs.

(1) La responsabilité du système de gestion des identités incombe à la haute direction ou à la gestion des affaires de l'organisation.

(2) Les processus et les systèmes de l'organisation qui attribuent des justificatifs d'identité aux utilisateurs (identifiants, mots de passe, jetons d'authentification, etc.) sont dotés des mesures appropriées de gestion du risque (pratiques de sécurité, contrôles lors d'un changement au niveau des cadres, pistes de vérification, imputabilité, etc.).

2.1 Pratiques en matière d'identification

2.1.1. En tant que fournisseur d'identités, l'organisation détermine qui peut obtenir une identité électronique.

Quel sous-ensemble de personnes inscrites dans le système de gestion des identités de l'organisation considérerait-on comme « actif » dans les confirmations envoyées aux autres participants?

Les employés et les étudiants inscrits dans divers programmes.

Les étudiants diplômés et certains employés retraités gardent un accès à leur compte courriel mais ne sont plus considérés comme actifs.

2.1.2. Les identifiants de longue durée, non réattribués et uniques revêtent une importance capitale pour la sécurité et la pérennité des activités des membres de la FCA.

Vous arrive-t-il de réattribuer des identifiants?

☒ Oui

☐ Non

Dans l'affirmative, veuille donner des précisions, comme le temps écoulé avant la réattribution.

J'ai indiqué « Oui » parce que nous n'avons pas de politique en place pour gérer ce genre de situation. Dans la pratique, nous utilisons des identifiants basés sur le prénom et le nom d'un utilisateur, rajoutant un chiffre dans les cas excessivement rare de collision. (Nous sommes une institution de très petite taille.) Comme les adresses courriel des étudiants ne sont jamais supprimées, il ne peut pas y avoir de réattribution dans ce cas. En plus de 10 ans en poste, je ne me souviens pas d'avoir vu un identifiant d'un ancien employé être réassigné à un nouvel employé ayant le même nom.

2.1.3. Les « attributs » sont des éléments d'information sur l'identité d'une personne conservés dans le système de gestion des identités. Ces éléments figurent dans la confirmation de la véracité des attributs fournie à d'autres participants (fournisseurs d'identités). La véracité des attributs doit être extrêmement fiable pour que vous puissiez adhérer à la FCA.

Selon vous, vos attributs sont-ils assez fiables pour…

…contrôler l'accès aux bases de données en ligne que l'organisation exploite sous licence?	☒ Oui ☐ Non
…servir à acheter des biens ou des services au nom de l'organisation?	☒ Oui ☐ Non
…donner accès à des renseignements personnels comme les relevés de notes des étudiants?	☒ Oui ☐ Non

3. Renseignements sur le fournisseur de services (Gestion fédérée des identités / eduroam)

Le fournisseur de services qui reçoit la confirmation de la véracité des attributs d'un participant respectera les politiques, les règles et les normes établies par ce dernier pour protéger et utiliser ses données. Les informations fournies ne serviront qu'aux fins pour lesquelles elles ont été remises.

On présume que le fournisseur de services ne demandera que les informations strictement nécessaires pour prendre la bonne décision concernant le contrôle des accès et n'utilisera pas l'information transmise à mauvais escient. Le fournisseur de services décrira ce sur quoi il s'appuie pour donner accès aux ressources qu'il gère et les pratiques qu'il applique aux attributs obtenus des autres participants.

3.1 Attributs

3.1.1. Quels renseignements réclamez-vous sur les attributs d'une personne? Veuillez décrire chaque service offert aux participants de la FCA séparément (un service par rangée).

Service	S'agit-il d'un service R&S?	Attributs requis	Motif	L'information est-elle partagée?
eduroam	S/O	**Jeu standard d'attributs RADIUS (annexe A du document** eduroam Compliance Statement**)** • référence temporelle de la demande d'authentification et de la réponse correspondante • identité EAP externe de la demande d'authentification (attribut User-Name) • identité EAP interne (identifiant réel de l'utilisateur) • adresse MAC du client établissant la connexion (attribut Calling-Station-Id) • réponse d'authentification (acceptée ou refusée)	Authentification	Non

Remarques. *Les attributs normalisés par eduroam ont été inscrits à l'avance afin que le document soit plus facile à remplir. Si vous n'offrez pas eduroam, veuillez supprimer cette rangée.*

Un service GFI de la catégorie d'entité Research & Scholarship (R&S) et les attributs qui s'y associent ont aussi été inscrits à titre d'illustration. Veuillez le supprimer et insérer vos propres données au besoin. Ajoutez des rangées au tableau s'il y a lieu.

3.2 Contrôles techniques

Les contrôles techniques servent à réguler l'accès aux données sensibles et l'exploitation de ces dernières. On s'attend à ce qu'ils s'appliquent à tous les services. S'il y a des exceptions, veuillez les décrire.

3.2.1. Décrivez les mesures humaines et techniques mises en place pour contrôler l'accès aux attributs susceptibles d'identifier une personne et leur utilisation.

Les comptes de nos utilisateurs sont des comptes Microsoft Office 365. Bien que les adresses courriel soient effectivement publique pour tous nos utilisateurs (en accédant au carnet d'adresse), aucun autre attribut n'est accessible. En particulier, aucun utilisateur ne peut avoir accès au mot de passe utilisé par un autre utilisateur. Pour des raisons de diagnostics, certains techniciens ont accès aux adresses IP des utilisateurs qui se connectent à nos systèmes et peuvent associer cette adresse IP à un compte informatique. Ces techniciens doivent accéder à nos systèmes en utilisant une authentification à facteurs multiples.

3.2.2. Décrivez les mesures humaines et techniques mises en place pour gérer les comptes des super utilisateurs et les autres comptes avec privilèges pouvant donner accès à des informations susceptibles de permettre l'identification d'une personne.

Les super utilisateurs doivent accéder à leur compte en utilisant une authentification à facteurs multiples.

3.2.3. Si des informations permettant d'identifier quelqu'un sont compromises, quelles mesures prenez-vous afin d'en aviser ceux que cela pourrait toucher?

Lorsque nous sommes avisés d'une telle situation, nous cherchons à aviser les utilisateurs ayant un compte compromis en utilisant une méthode secondaire (deuxième adresse courriel, appel téléphonique, ou communication verbale par un collègue les avisant de nous contacter).

3.3 Autres considérations

3.3.1. Quelles autres considérations ou informations aimeriez-vous signaler aux participants de la FCA avec lesquels vous pourriez interagir?

Rien à ajouter.