




canarie



 French (Canada) ▾

## Programme Initiatives en cybersécurité (PIC) – Inscription aux initiatives

---

Les organisations admissibles (OA) qui souhaitent participer au programme Initiatives en cybersécurité (PIC) sont d'abord tenues de conclure [l'Entente de collaboration en cybersécurité avec une organisation \(ECCO\)](#) de CANARIE.

Les informations fournies dans ce formulaire sont nécessaires à l'ECCO. Il sera plus facile de remplir le formulaire si vous prenez connaissance des parties surlignées dans le modèle de l'entente.

Une fois que l'organisation aura ratifié l'ECCO, un représentant du [partenaire du Réseau national de la recherche et de l'éducation \(RNRE\)](#) de votre région prendra contact avec vous pour vous expliquer comment accéder aux initiatives subventionnées.

**Attention** : les coordonnées des personnes-ressources seront transmises au partenaire du RNRE local de l'organisation.

Choisir la province ou le territoire.

Choisir ▾

## Renseignements sur l'organisation et ses personnes-ressources

---

### Nom légal de l'organisation \*

Exemple : le nom légal de l'Université de Lansdowne est « The Governors of the University of Lansdowne ».

### Instance où l'organisation est constituée en société. \*

Exemple : l'Université de Lansdowne a été constituée en société selon les lois du Canada ou « une institution d'enseignement constituée en vertu de la charte royale de 1872 et ses modifications ».

### Nature de l'organisation \*

Exemples : organisation sans but lucratif, société, institution de recherche sans but lucratif

## Personnes-ressources

Veillez fournir les renseignements pertinents sur l'organisation et les coordonnées des personnes-ressources tel qu'indiqué plus bas. Chaque contact recevra un exemplaire de la ou des ententes pertinentes après leur ratification.

**Attention** : les coordonnées des personnes-ressources fournies dans le formulaire seront transmises au partenaire du RNRE de la province ou du territoire concerné.

Une fois la ou les ententes ratifiées, un représentant du partenaire du RNRE de votre région prendra contact avec vous pour vous expliquer comment accéder aux initiatives subventionnées.

### Adresse de l'organisation \*

Rue

Rue (2e ligne)

Ville

État / Province

Code postal

**Nom du requérant \***

Prénom

Nom

**Titre du requérant \***

**Téléphone \***

Indicatif  
régional

Numéro (incluant le poste, s'il y a  
lieu)

**Courriel \***

exemple@exemple.com

## **Personne-ressource pour l'entente de collaboration en cybersécurité (ECCO)**

Veuillez indiquer la personne de l'organisation à contacter. Il devrait s'agir du dirigeant principal de l'information (DPI), de l'agent principal de la sécurité de

l'information (APSI) ou de leur équivalent. Voir le paragraphe 1. b (page 2) de [l'ECCO](#).

**Contact de l'organisation pour l'ECCO \***

Prénom

Nom

**Titre \***

**Téléphone \***

Indicatif régional

Numéro (incluant le poste, s'il y a lieu)

**Courriel \***

exemple@exemple.com

**L'adresse de cette personne est-elle identique à celle de l'organisation (fournie plus haut)? \***

Oui

Non

**Signataire autorisé pour l'ECCO**

Veuillez indiquer la personne autorisée à signer pour l'organisation. Il pourrait s'agir du DPI, d'un vice-président ou de leur équivalent. Lire le paragraphe section 1. c (page 2) de [l'ECCO](#).

**Attention** : cette personne doit pouvoir lier l'organisation juridiquement.

### Signataire autorisé de l'organisation pour l'ECCO \*

Prénom

Nom

### Titre \*

### Téléphone \*

Indicatif régional

Numéro (incluant le poste, s'il y a lieu)

### Signing Authority Email Address \*

exemple@exemple.com

L'adresse de cette personne est-elle identique à celle de l'organisation (fournie plus haut)? \*

- Oui
- Non

### Signataire autorisé supplémentaire ou suppléant pour l'ECCO

Le cas échéant, veuillez fournir les coordonnées de la personne qui Signataire autorisé supplémentaire ou suppléant. Il devrait s'agir du DPI, d'un vice-président ou de leur équivalent. Le nom du Signataire autorisé supplémentaire ou suppléant, s'il y en a un, apparaîtra au paragraphe 1. c (page 2) de [l'ECCO](#).

**Attention** : cette personne doit pouvoir lier l'organisation juridiquement.

Signataire autorisé supplémentaire ou suppléant : \*

- Aucun Signataire autorisé supplémentaire ou suppléant
- L'organisation a un signataire autorisé supplémentaire ou suppléant

**Remplaçant du signataire autorisé de l'organisation pour l'ECCO \***

Prénom

Nom

**Titre \***

**Téléphone \***

Indicatif régional

Numéro (incluant le poste, s'il y a lieu)

**Courriel \***

exemple@exemple.com

**L'adresse de cette personne est-elle identique à celle de l'organisation (fournie plus haut)? \***

- Oui
- Non

**Adresse du remplaçant du signataire autorisé \***

Rue

Rue (2e ligne)

Ville

État / Province

Code postal

## Choix d'une initiative subventionnée

Veillez choisir les initiatives subventionnées que l'organisation souhaite instaurer.

### Le CIRA DNS Firewall

Simple à installer, le CIRA DNS Firewall est un outil puissant qui mettra votre réseau à l'abri des menaces en ajoutant une couche de sécurité à celles que vous avez déjà mises en place. Le pare-feu :

- empêche l'utilisateur (et les robots de recherche) d'accéder aux sites malveillants susceptibles d'abriter des virus et des maliciels ou pratiquant l'hameçonnage;
- bloque les logiciels malveillants et les tentatives d'hameçonnage;
- agrège les données sur les menaces de façon à permettre ou à interdire l'accès en fonction des renseignements glanés en temps réel;
- signale les activités suspectes;
- atténue les risques en localisant et isolant les dispositifs infectés.

#### Le CIRA DNS Firewall

- Mon organisation souhaite s'inscrire au CIRA DNS Firewall.
- Mon organisation ne souhaite pas s'inscrire au CIRA DNS Firewall

### Fil de menaces du CanSSOC

Le Fil de menaces du CanSSOC fournit aux institutions de recherche et d'enseignement des informations précises au sujet des menaces qui planent sur leur secteur. Il agrège et structure les données des organisations de cybersécurité publiques et privées ainsi que des sources ouvertes en une liste d'interdictions et d'autorisations pouvant être directement déployée sur les pare-feu existants.

### **Pour les organisations du milieu de la recherche et de l'éducation, le Fil de menaces du CanSSOC :**

- renforce les protections existantes avec des informations exploitables adaptées aux institutions de recherche et d'enseignement;
- s'intègre facilement à la plupart des pare-feu de la prochaine génération (Palo Alto, Fortinet FortiGate et Cisco Firepower) pour bloquer automatiquement les adresses IP, les URL et les domaines malveillants;
- réduit les coûts en exploitant les renseignements et les fils d'information disponibles sur le marché;
- autorise, si on le désire, le renvoi des données sur les menaces au CanSSOC en vue de mieux renseigner l'ensemble du secteur.

#### **Fil de menaces du CanSSOC**

- Mon organisation souhaite s'inscrire au Fil de menaces du CanSSOC.
- Mon organisation ne souhaite pas s'inscrire au Fil de menaces du CanSSOC.

#### **Fil de menaces du CanSSOC – Étapes suivantes**

Une fois que l'organisation aura conclu l'ECCO avec CANARIE, son signataire autorisé recevra **l'Entente de confidentialité du CanSSOC..**

Pour préparer l'Entente de confidentialité du CanSSOC, nous avons besoin des renseignements que voici :

1. Coordonnées du contact principal en cybersécurité. Il participera à une séance d'information technique d'environ deux (2) heures en prévision de l'installation du Fil de menaces. Cette séance a habituellement lieu quatre à douze semaines après la ratification de l'entente.
2. Coordonnées du signataire autorisé pour l'Entente de confidentialité du CanSSOC.



Après ratification de l'entente, le partenaire du RNRE de votre région communiquera avec vous pour organiser la séance d'information précédant l'installation du Fil de menaces.

**Contact principal en cybersécurité pour le Fil de menaces du CanSSOC \***

Prénom

Nom

Titre

**Téléphone**

Indicatif régional

Numéro (incluant le poste, s'il y a lieu)

**Courriel**

exemple@exemple.com

Sélectionnez le pare-feu qu'alimentera le Fil de menaces du CanSSOC.

Autre – indiquer le nom du pare-feu

**Signataire autorisé pour l'Entente de confidentialité du CanSSOC**

Veuillez indiquer la personne autorisée à signer l'entente pour l'organisation.

**Attention** : cette personne doit pouvoir lier l'organisation juridiquement.

Le signataire autorisé pour l'Entente de confidentialité du CanSSOC est-il identique au signataire autorisé pour l'ECCO de CANARIE indiqué plus haut?

Le signataire autorisé de l'organisation recevra l'ECCO de CANARIE par DocuSign.

**Si vous avez choisi le CIRA DNS Firewall.**

- Après la ratification de l'ECCO, le partenaire du RNRE de votre région vous enverra un lien menant au portail de la CIRA afin que vous puissiez commencer à configurer le pare-feu.

**Si vous avez choisi le Fil de menaces du CanSSOC.**

- Après la ratification de l'ECCO, le signataire autorisé de l'organisation recevra une copie de l'Entente de confidentialité du CanSSOC par DocuSign.
- Après la ratification de l'Entente de confidentialité du CanSSOC, le partenaire du RNRE de votre région communiquera avec le contact principal en cybersécurité de l'organisation pour organiser la séance d'information technique sur le Fil de menaces.

**Si vous avez choisi le SDI.**

- L'équipe CANARIE enverra l'Entente de participation au SDI au signataire autorisé de l'organisation.
- Après la ratification de l'entente par les deux parties, nous communiquerons avec le contact technique en cybersécurité mentionné plus haut pour organiser la séance d'information durant laquelle on lui expliquera l'initiative et on le guidera dans le choix de l'équipement à commander. De cette façon, vous sélectionnez la configuration du serveur SDI qui convient le mieux à l'infrastructure de l'organisation.
- L'équipe CANARIE enverra le formulaire pour commander l'équipement SDI au contact technique en cybersécurité de l'organisation. Une fois soumis, le bon de commande sera automatiquement envoyé à Bell, le distributeur du matériel retenu.
- L'équipe CANARIE assurera le suivi afin d'organiser une séance de formation sur l'installation, la configuration et l'utilisation du SDI.

Vous pouvez écrire à [cip \(@\) canarie.ca](mailto:cip (@) canarie.ca) pour connaître l'avancement de vos demandes sur les initiatives du PIC.