Plan d’activités annuel de CANARIE

2026-2027 (EF27)

Le 30 Janvier 2026

canarie.ca

Table des matières

1. Aperçu

CANARIE a le plaisir de présenter son plan d'activités pour l'exercice 2026-2027 (EF27), deuxième année du mandat qui court de 2025 à 2030. Le document que voici explique comment l'organisation entend atteindre les résultats souhaités durant l'exercice, les risques auxquels elle s'expose et les stratégies qu'elle a échafaudées pour les atténuer.

1.1 Rôle de CANARIE

CANARIE et ses treize partenaires provinciaux et territoriaux forment le Réseau national de la recherche et de l'éducation (RNRE) canadien, un réseau ultrarapide qui connecte les scientifiques et les membres du personnel enseignant du Canada entre eux et leur donne accès à leurs homologues, aux données et aux technologies du monde entier.

Afin de rendre le milieu canadien de la recherche et de l'éducation plus sûr, CANARIE finance, met en œuvre et soutient des initiatives en cybersécurité avec la collaboration de ses partenaires du RNRE, du gouvernement, des établissements d'enseignement supérieur et du secteur privé. L'organisation procure aussi des services de gestion des identités au milieu collégial et universitaire grâce à eduroam, de même que ses propres services de gestion des identités et des accès.

Fondé en 1993, CANARIE est une société sans but lucratif principalement financée par le gouvernement du Canada.

1.2 Vision et principes directeurs pour le mandat de 2025-2030

La vision retenue par CANARIE pour son mandat de 2025 à 2030 est celle d'« Un Canada mieux protégé et plus novateur ».

La stratégie adoptée eu égard au fonctionnement du réseau consiste à faire en sorte qu'à long terme, le réseau CANARIE évolue et se développe d'une manière souple et rentable par le déploiement de fibres optiques à la grandeur du pays. De cette façon, l'organisation disposera de la marge de manœuvre nécessaire pour accroître les capacités du réseau et implanter rapidement les technologies transformatrices à un coût considérablement moindre, surtout face à l'expansion notable du trafic qu'on prévoit dans l'avenir. Les progrès technologiques comme l'usage de satellites à orbite basse et la location de services de connexion rehausseront la connectivité et apporteront la diversité requise au réseau tout en élargissant sa portée. CANARIE facilite aussi l'accès à son réseau en orchestrant l'évolution du réseau fédéré canadien, soit le Réseau national de la recherche et de l'éducation (RNRE), et en procurant aux scientifiques du pays les services de gestion des identités et des accès (GIA) dont ils ont besoin pour profiter en toute sécurité des données, des infrastructures et des outils mis à leur disposition, partout dans le monde.

Sur le plan de la cybersécurité, CANARIE propose un éventail d'outils et de services et assure une coordination nationale qui aident le milieu canadien de la recherche et de l'éducation à mieux se protéger et à accroître sa résilience selon le principe de la « cybersécurité collective ».

Pour atteindre cet objectif, CANARIE articulera ses activités en cybersécurité sur les cinq axes que voici :

(1) en évaluant et en priorisant les risques courus par la communauté (au moyen de l'Évaluation nationale de la cybersécurité, de l'Analyse comparative des vulnérabilités et ainsi de suite);

(2) en rassemblant, analysant et diffusant des informations exploitables sur les menaces (par le Fil de menaces et la surveillance du web clandestin, par exemple);

(3) en synchronisant les activités, en triant les cyber incidents et en y réagissant plus vite (grâce au SOC fédéré du CanSSOC, dont l'essai vient de se terminer et dont on attend le financement intégral par le gouvernement canadien);

(4) en regroupant et en partageant les ressources (sous la forme de modèles, de cadres, de contenu, etc. communs);

(5) en mobilisant la collectivité.

1.3 Nature des activités au cours de l'EF27 (du 1er avril 2026 au 31 mars 2027)

Gestion et évolution continues de son réseau et d'autres programmes mises à part, voici les principales activités que CANARIE envisage au cours de l'EF27 pour étayer sa vision d'un « Canada mieux protégé et plus novateur » et leurs résultats.

- Continuer d'accroître le débit du réseau CANARIE pour le porter à 400 Gbps
- Établir une connexion directe vers la région de l'Asie-Pacifique afin de soutenir la recherche mondiale
- Lancer le deuxième appel à projets du programme RNRE en vue de raccorder au réseau les groupes qui ne le sont pas encore, plus particulièrement les institutions autochtones
- Élargir l'éventail des services d'identification en misant sur la gestion fédérée des identités avec le déploiement d'un service géré
- Poursuivre l'évolution du programme Initiatives en cybersécurité (PIC) et l'optimiser en fonction des résultats visés au niveau des cinq axes stratégiques
- Continuer à coordonner ses activités avec celles de l'Alliance de la recherche numérique du Canada pour appuyer la stratégie du gouvernement canadien relative à l'infrastructure de recherche numérique

2. Réalisations en 2025-2026

L'année 2025-2026 (EF26) était la première du mandat de CANARIE de 2025 à 2030. Les pages qui suivent brossent un tableau général de ce qui a été accompli jusqu'à présent dans les deux champs d'activité admissibles que mentionne l'Accord de contribution régissant ce mandat. S'y ajoutent des informations sur les projets en cours, en voie d'achèvement. Voici ce que CANARIE a réalisé pour l'instant, durant l'EF26.

- L'organisation a élaboré un modèle fédéré national qui tiendra la collectivité au courant de la situation avec la réussite du projet pilote de centre des opérations en sécurité (SOC) fédéré du CanSSOC.
- Elle a soumis au gouvernement du Canada une proposition le priant de financer le SOC fédéré du CanSSOC et d'en faire un des principaux services que dispensera CANARIE à partir du 1er avril 2026.
- Elle a modernisé le matériel optique du réseau le long du corridor entre Winnipeg, Thunder Bay et Sudbury afin de répondre aux besoins de connectivité du milieu de la recherche et de l'éducation (R-E).
- Elle a organisé l'édition 2025 du Forum SecuR&E dont l'objectif consiste à renforcer la communauté et à favoriser l'apprentissage ainsi que le partage du savoir en rassemblant ceux et celles qui concourent à la cybersécurité du milieu R-E, au Canada.
- Elle a sélectionné puis sanctionné les projets qui seront financés dans le cadre du premier appel à projets du RNRE et permettront au RNRE d'instaurer des infrastructures réseau et de sécurité, de les agrandir ou de les améliorer, ainsi que de perfectionner et de retenir les éléments talentueux.
- Elle a diffusé les documents de l'analyse des investissements en cybersécurité et le plan qui s'y rattache à la communauté en vue d'établir un point de référence national sur les sommes que le secteur R-E canadien injecte dans la cybersécurité ainsi que de mieux cerner dans quoi investir davantage et où réaliser de plus grandes économies.
- Elle a fait du « fournisseur de service eduroam en tant que service » une fonction essentielle d'eduroam afin d'en faciliter le déploiement ailleurs que dans les établissements de recherche et d'éducation.
- Elle a créé un bulletin mensuel d'information technique en cybersécurité pour renseigner les équipes chargées de la sécurité dans les institutions.

Les principaux projets qui devraient s'achever ou démarreront avant la fin de l'EF26 sont les suivants :

- finir de remplacer l'équipement au MOXY, point d'échange international de CANARIE à Montréal, pour amener le débit de la liaison transatlantique à 400 G;
- organiser une séance d'information annuelle sur les questions de défense, de planification stratégique et de budget pour la direction des institutions;

- mettre sur pied le Centre de collaboration communautaire en cybersécurité afin de faciliter le regroupement et le partage des ressources dans tout le secteur R-E canadien.

Le rapport annuel de l'EF26, que ISDE recevra en juillet prochain, présentera le reste des réalisations de l'exercice 2025-2026.

3. Activités prévues en 2026-2027

L'EF27 constitue la deuxième année du mandat de 2025-2030 de CANARIE. Pour atteindre les résultats souhaités, l'organisation entreprendra les activités décrites plus bas, en 2026-2027:

3.1 Exploitation du réseau

CANARIE poursuivra toutes les activités requises pour soutenir son réseau et les services qui s'y rattachent, et en permettre l'évolution.

3.1.1 Programme Réseau

Durant l'EF27, le réseau CANARIE continuera de fonctionner et de se développer comme devrait le faire une infrastructure scientifique indispensable à la recherche, à l'éducation et à l'innovation:

Activités durant l'EF27	Résultats à court et à moyen terme pour l'EF27
▪ Exploiter le réseau ▪ En accroître les capacités, la redondance et la fiabilité ▪ En rehausser la surveillance par l'adoption de nouveaux outils	▪ Déploiement de capacités supplémentaires pour soutenir la croissance du trafic, notamment par la hausse du débit à 400 Gbps un peu partout au pays et l'introduction de services de 100 Gbps dans la région de l'Atlantique ▪ Amélioration des capacités su réseau dans le nord
▪ Protéger le réseau et l'organisation en adoptant des moyens pour prévenir, détecter et combattre les cybermenaces et ainsi préserver l'intégrité, la confidentialité et la disponibilité des données et des systèmes ▪ Continuer à rendre le réseau plus sûr ▪ Moderniser le système de détection des dénis de service distribué (DDoS) qui arrive en fin de vie	▪ Amélioration des rapports sur la sécurité du réseau, de la surveillance de cette dernière et des moyens permettant de la quantifier
▪ Poursuivre l'automatisation du réseau ▪ Continuer d'échafauder des stratégies pour améliorer l'efficacité, la fiabilité et la sécurité	▪ Déploiement d'applications qui automatiseront le réseau et poursuite des travaux sur son automatisation

des activités sur le réseau grâce à l'intelligence artificielle (IA)	▪ Échafaudage de plans afin de profiter de l'IA dans l'exploitation du réseau
▪ Continuer d'améliorer l'accès des utilisateurs au réseau grâce à des outils d'aide	▪ Déploiement d'outils d'aide accessibles sur le portail des utilisateurs
▪ Participer aux activités internationales en réseautique, notamment l'usage de satellites à orbite basse (SOB), la connectivité dans les régions polaires, la connectivité dans la région Asie-Pacifique et le groupe GNA-G (*Global Network Advancement Group*)	▪ Établissement de connexions directes dans la région Asie-Pacifique pour faciliter la recherche dans le monde

3.1.2 Programme Extension des infrastructures (PEI)

Au cours de l'EF27, CANARIE aidera les instituts de recherche du gouvernement à tirer parti du réseau de recherche pour faciliter la collaboration scientifique avec leurs partenaires du Canada et de l'étranger jusqu'à ce qu'ils soient raccordés au réseau de Services partagés Canada (SPC) à la fin de l'EF28.

Activités durant l'EF27	Résultats à court et à moyen terme pour l'EF27
▪ Maintenir la connexion à haute vitesse au réseau dans les installations de recherche du gouvernement	▪ Maintien des connexions existantes dans les installations de recherche du gouvernement afin de satisfaire aux exigences de rendement du personnel scientifique de la fonction publique
▪ Planifier le transfert de propriété des connexions existantes (connexions du PEI) au réseau scientifique du gouvernement canadien (RSGC) de Services partagés Canada (SPC)	▪ Transfert homogène des connexions en coordination avec SPC

3.1.3 Gestion des identités et des accès

Pendant l'FE27, CANARIE procurera des services de gestion des identités et des accès solides avec lesquels on pourra accéder à distance et en tout temps aux ressources et aux outils répartis d'une manière sûre et efficace, grâce à son programme « Fédération canadienne d'accès » (FCA).

Activités durant l'EF27	Résultats à court et à moyen terme pour l'EF27
▪ Continuer à collaborer avec les participants de la FCA et les spécialistes de l'industrie afin de planifier l'évolution du service ▪ Augmenter le nombre de lieux publics qui diffusent eduroam pour multiplier les possibilités d'apprentissage à distance et permettre un usage créatif des espaces communautaires ▪ Élargir l'éventail des services d'identification en proposant le déploiement de la gestion fédérée des identités comme service géré ▪ Collaborer avec la communauté internationale pour faire évoluer les services de gestion des identités	▪ Maintien de la forte participation à la FCA ▪ Hausse du nombre annuel de connexions à eduroam ▪ Augmentation du nombre de projets visant à accroître les capacités de la Fédération ▪ Augmentation du nombre d'interfaces, d'applications et d'outils qui soutiennent les services de la FCA ▪ Meilleure mobilisation de la collectivité par le partage des connaissances sur la GIA

3.1.4 Programme RNRE

Durant l'EF27, CANARIE continuera de développer le RNRE pour qu'il fonctionne de façon coordonnée et fasse progresser les objectifs communs tout en respectant la diversité du modèle fédéré et en tirant parti des avantages qui en découlent.

Activités durant l'EF27	Résultats à court et à moyen terme pour l'EF27
▪ Connecter au réseau les groupes qui ne le sont pas encore, plus particulièrement les institutions autochtones ▪ Renforcer la collaboration au sein du RNRE ▪ Améliorer les capacités, la redondance, la fiabilité et la sécurité du RNRE par le truchement des réseaux des partenaires provinciaux et territoriaux	▪ Lancement du deuxième appel à projets du RNRE en vue de raccorder au réseau les groupes qui ne le sont pas encore, surtout les institutions autochtones ▪ Exécution des projets retenus lors du premier appel du RNRE en vue de créer, d'élargir ou d'améliorer les infrastructures réseau et de sécurité ainsi que de perfectionner et de retenir les éléments talentueux ▪ Planification du lancement du troisième appel à projets du RNRE visant la création, l'agrandissement ou l'amélioration des infrastructures réseau ou de sécurité ainsi que

	le perfectionnement et la rétention des éléments brillants ▪ Exécution des projets de protection du routage, modernisation et implantation des outils de surveillance PerfSONAR ainsi qu'introduction de moyens pour quantifier la sécurité du RNRE et collecte des données pertinentes sous la coordination de CANARIE

3.2 Cybersécurité

Au cours de l'EF27, CANARIE s'efforcera d'améliorer la cybersécurité générale du milieu de la recherche et de l'éducation:

Activités durant l'EF27	Résultats a court et à moyen terme pour l'EF27
▪ Identifier, prioriser puis mettre en œuvre des initiatives en cybersécurité d'après les données, les réalités et les risques analysés à la grandeur du secteur, notamment la revue des programmes et des services existants afin de garantir leur utilité pour la communauté et de mieux rationaliser le modèle d'exécution	▪ Initiatives en cybersécurité élaborées de plus en plus en fonction des données, de l'analyse des risques et des réalités sectorielles pour qu'on investisse de façon plus judicieuse en prévision d'un impact plus prononcé ▪ Adhésion accrue à des services de cybersécurité d'une plus grande utilité pour les participants et réduction des obstacles qui entravent une telle participation
▪ Continuer de faire progresser le Fil de menaces du CanSSOC pour en faire un vaste service national de renseignement sur les menaces en y ajoutant des indicateurs techniques, des séances d'information contextuelles, des avis sur les Nouvelles menaces et des règles de détection automatique	
▪ Terminer la quatrième édition de l'Évaluation nationale de la cybersécurité (ENC) en y apportant des améliorations opérationnelles et stratégiques ▪ Profiter du succès remporté par l'ENC pour y inclure une série de services de modélisation des cyber risques plus stratégique et les modèles qui en dérivent	▪ Meilleures coordination, collaboration et interventions collectives sur les risques les plus prioritaires dans le milieu R-E s'appuyant sur un meilleur partage des connaissances
▪ Agrandir le nouveau portail de collaboration sectoriel afin de diffuser au moment opportun du contenu en cybersécurité stratégiquement	▪ Adoption générale des modèles normalisés, des cadres et des ressources opérationnelles grâce à l'enrichissement de la bibliothèque

utile et exact, adapté au milieu R-E, notamment en autorisant l'apport de contenu par la collectivité et la formulation de commentaires par des pairs	commune du portail en vue de réduire les efforts inutiles et de parvenir à une plus grande cohérence dans le secteur
▪ Repenser le modèle consultatif en cybersécurité de CANARIE pour garantir une participation plus directe de la collectivité sur les plans stratégique et technique ▪ Élargir la diffusion des bulletins de renseignement techniques et organiser une séance d'information annuelle sur les menaces pour les cadres supérieurs ainsi que lancer une série de webinaires sur la cybersécurité afin de partager l'information et de renforcer la prise de décisions dans les institutions	▪ Participation accrue et meilleur alignement des dirigeants de la communauté en vue de parvenir à un partenariat plus fiable et de mieux étayer les priorités en cybersécurité

3.3 Activités entreprises avec l'Alliance de la recherche numérique du Canada

Au cours de l'EF27, CANARIE collaborera avec l'Alliance de la recherche numérique du Canada (ARNC) pour aider le gouvernement canadien à mettre à exécution sa stratégie sur l'infrastructure de recherche numérique.

Activités durant l'EF27	Résultats à court et à moyen terme pour l'EF27
▪ Intégrer les outils et les services de CANARIE et de l'ARNC, dont ceux en cybersécurité	▪ Meilleure intégration de la gestion fédérée des identités aux services de l'ARNC ▪ Soutien des besoins en réseautique du centre de données de l'ARNC par CANARIE ▪ Participation de l'ARNC et des sites d'hébergement aux services de cybersécurité de CANARIE, notamment à l'Évaluation nationale de la cybersécurité
▪ Continuer d'harmoniser les activités de gouvernance, de communication et de rayonnement ▪ Examiner les moyens d'appuyer la science au sein du gouvernement canadien, y compris les ministères et les organismes à vocation scientifique ainsi que les politiques scientifiques fédérales	▪ Alignement des deux organisations au niveau de la gouvernance en cybersécurité, notamment en confiant la présidence de leurs comités de cybersécurité à une seule et même personne

3.4 Activités contribuant à l'équité, à la diversité et à l'inclusion

Pendant l'EF27, CANARIE s'efforcera de faire progresser l'équité, la diversité et l'inclusion (EDI) à l'interne et dans les programmes que l'organisation a mis en place.

Activités durant l'EF27	Résultats à court et à moyen terme pour l'EF27
▪ Soutenir les groupes mal servis au Canada et à ailleurs dans le monde ▪ Poursuivre la stratégie et les activités qui encouragent la participation des Autochtones ▪ Continuer d'utiliser les plans EDI des institutions comme critère pour sélectionner les projets qui seront financés, quand la chose est appropriée	▪ Lancement du deuxième appel à projets visant à raccorder au RNRE les institutions qui ne le sont pas encore, particulièrement les institutions autochtones ▪ Participation aux consortiums qui posent un câble sous-marin dans l'Arctique et recours aux SOB pour mieux connecter la population dans le Nord
▪ Former le personnel de CANARIE sur les sujets qui feront avancer l'EDI	▪ Soutien constant des groupes d'entraide du personnel de CANARIE

▪ Continuer à passer en revue les politiques, les procédures et les pratiques de l'organisation	▪ Formation supplémentaire dispensée au personnel, au besoin

4. Échéancier d’exécution des programes

		Exercice 2026-2027			
Activités admissibles	**Initiatives**	**En cours**	**Lancement prévu ou *réel***	**Principaux jalons (antérieurs)**	**Achèvement prévu (antérieur)**
Exploitation du réseau					
Programme Réseau	Exploiter le réseau				
	En accroître les capacités, la redondance et la fiabilité - Jalon 6 : matériel optique installé sur le tronçon Est - Jalon 7 : service de 400 Gbps lancé sur le tronçon Est, débit porté à 400 Gbps à l'ouest et au sud de Montréal - Jalon 8 : ancien équipement retiré et nettoyage **Fin du projet de modernisation du réseau**		***2020-04-01***	***2025-10-24*** **(2025-08-22)** ***2025-01-16*** **(2025-09-26)** **2026-02-20 (2025-11-28)**	**2026-02-20 (2025-11-28)**
	En augmenter les capacités, la redondance et la fiabilité Lancer des demande de propositions (DP) pour de l'équipement - Augmenter le débit des services gérés de 100 à 400 Gbps - Porter le débit des services gérés de 10 à 100 Gbps dans la région de l'Atlantique - Porter le débit du service géré à 1 Gbps dans les Territoires du Nord-Ouest		**2026-04-01**	**2026-05-08** **2026-06-19** **2026-05-08**	**2027-03-26** **2026-10-30** **2026-08-21**
	Continuer de perfectionner les outils servant à mieux protéger le réseau et à en suivre l'utilisation				
	Poursuivre le développement des services réseau virtuels - Jalon 1a : démonstration de la plateforme réseau virtuelle - Jalon 2 : inventaire du réseau dressé par la plateforme - Jalon 3 : illustration de la configuration du réseau par la plateforme - Jalon 4 : démonstration scientifique de la configuration du réseau par la plateforme au colloque SuperComputing de 2026		***2023-04-01***	***2025-03-28*** **(2025-05-30)** **2026-05-29 (2025-09-26)** **2026-09-18 (2026-02-26)** **2026-11-15**	**2030-03-31**
	Participer aux activités internationales de réseautique - Conclure une entente en vue d'établir une liaison directe entre le Canada et la région Asie-Pacifique		**2026-04-01**	**2026-07-01**	**2027-03-12**

Activités admissibles	Initiatives	En cours	Lancement prévu ou *réel*	Principaux jalons (antérieurs)	Achèvement prévu (antérieur)
Programme Réseau (suite)	Mettre à niveau le système de détection des attaques par déni de service distribué (DDoS) du réseau CANARIE **Initiative reportée d'un an en raison des contraintes budgétaires** - Jalon 1 : choisir un fournisseur pour l'équipement et les services - Jalon 2 : nouveau système DDoS mis en service - Jalon 3 : réglages terminés, début de la production		**2026-04-01 (2025-04-01)**	**2026-08-28 (2025-08-29)** **2026-11-27 (2025-11-28)** **2027-03-19 (2026-02-27)**	**2027-03-19 (2026-02-27)**
	Surveiller la cybersécurité sur l'infrastructure, le services et le réseau CANARIE; laisser les partenaires du RNRE surveiller la cybersécurité sur leur propre réseau				
	Utiliser le système de détection des attaques DDoS réservé au réseau CANARIE et collaborer activement avec les partenaires du RNRE				
	Promouvoir et faciliter le perfectionnement en cybersécurité du personnel pertinent de CANARIE à l'interne et celui des analystes en sécurité du RNRE				
Programme PEI	Procurer une connexion ultrarapide aux installations de recherche du gouvernement - Jalon 1 : planifier le transfert des connexions existantes de CANARIE à SPC		***2025-04-01***	**2026-03-27 (2025-06-27)**	**2027-03-31**

Activités admissibles	Initiatives	En cours	Lancement prévu ou *réel*	Principaux jalons (antérieurs)	Achèvement prévu (antérieur)
Programme Gestion des identités et des accès	Promouvoir l'adoption de l'outil CAT (*Configuration Assistant Tool*) d'eduroam qui crée des profils pour accroître la sécurité au sein de la communauté				
	Élaborer une documentation technique plus solide et des tutoriels pour simplifier le déploiement, l'application et l'utilisation d'eduroam et des services de GIA				
	Promouvoir la technologie des services gérés qui facilite le déploiement d'eduroam pour augmenter le nombre de lieux qui offrent ce service à la population				
	Appliquer une technologie des services gérés comme celle d'eduroam à la gestion des identités et des accès dans la communauté - Jalon 1 : technologie sélectionnée - Jalon 2 : mise à l'essai dans quelques institutions - Jalon 3 : technologie des service gérés prête à être déployée		***2024-08-07***	***2025-01-30*** ***2025-04-03*** ***2025-10-31*** **(2025-08-22)**	**2025-02-27** **(2025-09-26)**
	Évaluer les besoins de la communauté en gestion des identités et des accès - Jalon 1 : fournisseur sélectionné pour l'étude du marché - Jalon 2 : résultats préliminaires obtenus - Jalon 3 : convertsion des résultats en composantes d'une communauté de pratique en GIA et adaptation du programme de CANARIE en conséquence		**2025-03-04**	***2025-06-27*** ***2025-12-19*** **(2025-12-12)** **2026-02-27**	**2026-03-27**
	Accroître la disponibilité d'eduroam, donc son usage et son utilité (dans un plus grand nombre d'aérogares, par exemple) - Jalon 1 : consultation des aéroports sélectionnés terminée		**2026-04-01**	**2026-06-26**	**2026-03-27**
Programme RNRE	1er appel à projets - Jalon 1 : charte de l'appel approuvée - Jalon 2 : lancement de l'appel aux partenaires du RNRE - Jalon 3 : sélection des projets		***2025-01-13***	***2025-01-30*** ***2025-04-03*** ***2025-10-08***	**2028-01-31**
	2e appel à projets - raccordement des groupes non connectés - Jalon 1 : charte de l'appel approuvée - Jalon 2 : lancement de l'appel aux partenaires du RNRE - Jalon 3 : sélection des projets		**2025-07-01**	***2025-12-23*** **(2025-12-12)** **2026-04-02** **2026-11-02**	**2029-01-31**
	3e appel à projets - Jalon 1 : charte de l'appel approuvée - Jalon 2 : lancement de l'appel aux partenaires du RNRE - Jalon 3 : sélection des projets		**2026-02-02**	**2026-03-27** **2026-06-05** **2026-11-20**	**2029-01-31**

Activités admissibles	Initiatives	En cours	Lancement prévu ou *réel*	Principaux jalons (antérieurs)	Achèvement prévu (antérieur)
Cybersécurité	Poursuivre le Fil de menaces, l'Évaluation nationale de la cybersécurité et l'Analyse comparative des vulnérabilités pour les organisations admissibles intéressées				
	Projet pilote de SOC fédéré du CanSSOC - Jalon 3 : collecte des données terminée - Jalon 4 : proposition soumise à ISDE		***2023-09-03***	***2025-06-30*** ***2025-09-12***	**2026-08-28**
	Évaluer le partage des informations sur la plateforme de collecte de données de l'ENC en vue de l'améliorer - Jalon 1 : choix d'un fournisseur - Jalon 2 : plateforme améliorée en prévision de la 4e édition de l'ENC		***2025-04-01***	***2025-12-19*** **(2025-07-25)** **2026-03-27** **(2025-10-31)**	**2026-03-31**
	Évaluer le partage des informations après la collecte des données de la 4e édition de l'ENC - Jalon 1 : données recueillies Ajouter un service de modélisation des cyber risques - Jalon 1 : choix d'un fournisseur pour la gestion des risques par un tiers (GRT) - Jalon 2 : essai de la gestion des risques par un tiers (GRT) terminé		***2025-12-22***	**2026-06-12** ***2025-10-31*** **2026-08-28**	**2026-07-31** **2027-03-26**
	Centre des opérations en sécurité (SOC) fédéré du CanSSOC - Jalon 1 : financement confirmé - Jalon 2 : 30 institutions ajoutées au projet - Jalon 3 : service opérationnel en tout temps planifié		**2026-04-01**	**2026-06-12** **2027-03-26**	**2027-03-31**
	Faire progresser le Fil de menaces du CanSSOC - Jalon 1 : reproduction du fil de menaces de l'Université McGill à CANARIE - Jalon 2 : fil perfectionné et opérations quotidiennes transférées de l'université à CANARIE - Jalon 3 : intégration d'autres indicateurs techniques, de bulletins contextuels et de renseignements sur les nouvelles menaces		***2025-04-01***	***2025-09-26*** **2026-02-20** **2026-06-26**	**2026-03-31** **2026-11-27**
	Augmenter le contenu en cybersécurité offert sur le portail de collaboration - Jalon 1 : contenu minimal sur le sujet établi et intervalle de mise à jour modifié - Jalon 2 : ajout des premiers contenus fournis par la communauté		**2026-04-01**	**2026-08-28** **2027-03-20**	**2027-03-31**
	Multiplier les mises à jour techniques en cybersécurité - Jalon 1 : série de webinaires Horizons SecuR&E lancée		**2026-04-01**	**2026-05-04**	**2027-03-31**

Activités admissibles	Initiatives	En cours	Lancement prévu ou *réel*	Principaux jalons (antérieurs)	Achèvement prévu (antérieur)
Activités entreprises avec l'Alliance de recherche numérique du Canada					
Cybersécurité	Utilisation de l'Évaluation nationale de la cybersécurité (ENC) par l'Alliance et les sites d'hébergement - Jalon 1 : choix d'un administrateur responsable du questionnaire de l'ENC aux sites d'hébergement - Jalon 2 : inscription à l'ENC		***2025-04-01***	**2026-02-27 (2025-07-31)** **2026-04-24 (2025-09-30)**	**2026-05-29 (2026-02-27)**
	Alignement des deux organisations au niveau de la gouvernance en cybersécurité, y compris présidence des deux comités de cybersécurité par une seule et même personne				
	Poursuite du travail en vue d'intégrer la gestion fédérée des identités aux services CIP de l'Alliance				
Activités contribuant à l'équité, à la diversité et à l'inclusion					
EDI	2e appel à projets pour raccorder au RNRE les groupes qui ne le sont pas encore, y compris les institutions autochtones		*Voir le 2e appel à projets du RNRE*	*Voir le 2e appel à projets du RNRE*	*Voir le 2e appel à projets du RNRE*
	Poursuite des activités avec les consortiums qui posent un câble sous-marin dans l'Arctique afin d'améliorer la connectivité dans le Nord				
	Soutien constant des groupes d'entraide du personnel de CANARIE				
	Formation supplémentaire pour le personnel				

5. Assertion et plan financier

Le gouvernement du Canada a débloqué 176 M$ pour financer les activités de CANARIE de 2026 à 2030. Grâce à ces fonds, CANARIE continuera d'investir de façon stratégique dans son infrastructure et les services qu'il met à la disposition des scientifiques et des personnes qui innovent au pays. Comme le veut l'Accord de contribution, 31,9 M$ serviront à financer les activités de l'organisation durant l'EF27 et CANARIE s'engage à préserver, à investir, à administrer et à utiliser ces fonds comme le stipule l'Accord de contribution.

5.1 Revenus et dépenses

Le tableau qui suit résume les revenus et les dépenses prévus au titre des programmes de CANARIE pendant l'EF27.

	(en milliers $)
Revenus	
Financement	
Gouvernement du Canada	31 900
Sous-total	**31 900**
Rentrées	
Droits de participation	650
Intérêts	50
Sout-total	**700**
Revenus totaux	**32,600**
Dépenses	
Programmes	
Exploitation du réseau	
Infrastructure et services	15 645
RNRE	1 070
FCA	2 089
Sous-total	**18 804**
Cybersécurité	
Programmes et services	6 126
SOC fédéré du CanSSOC (projet pilote)	1 877
Sous-total	**8 003**
Dépenses (programmes)	**26 807**
Administration	5 793
Dépenses totales	**32 600**
Excédent	-

5.2 Financement

Tel qu'indiqué ci-dessus, CANARIE sollicite un montant de 31,9 M$ du gouvernement canadien pour l'EF27.

5.3 Assertion

CANARIE affirme ne déroger à aucune des conditions de l'Accord de contribution actuellement en vigueur.

5.4 Recouvrement des coûts

Le tableau que voici indique les coûts que CANARIE prévoit recouvrer au cours de l'EF27.

	(en milliers $)
Programmes (espèces)	
Droits d'utilisation du PEI – gouv. fédéral	100
Droits d'utilisation du PEI – autres établissements	6
Droits d'adhésion	544
Sous-total	**650**
Fonds de contrepartie	
Connectivité dans le Nord	860
Sous-total	**860**
RECOUVREMENT TOTAL	**1 510**

Au cours de l'EF27, CANARIE continuera de percevoir des droits d'utilisation pour certains de ses programmes et services.

- Dans le cadre du Programme d'extension des infrastructures (PEI) patrimonial, CANARIE absorbe le coût de la connexion des laboratoires du gouvernement fédéral et d'autres laboratoires au RNRE. La somme recouvrée pour raccorder les établissements fédéraux au réseau correspond à un montant fixe, versé annuellement par Services partagés Canada en compensation du coût annuel d'une telle connexion. Pour les établissements non fédéraux qui bénéficient du PEI, le montant inscrit au budget correspond au recouvrement total des dépenses prévues.

- Les droits d'adhésion correspondent aux frais recouvrés dans le cadre du programme FCA et d'autres initiatives du programme Réseau.

- Dans le cadre de l'initiative visant à raccorder le Nunavut au Réseau national de la recherche et de l'éducation, CANARIE assume le coût de la connexion du Collège de l'Arctique du Nunavut (CAN) et des communautés du territoire au réseau par des satellites à orbite basse, le raccordement par fibres optiques étant irréalisable pour l'instant. L'entente conclue entre CANARIE et le CAN prévoit un financement de contrepartie dans la proportion de 3:7.

5.5 Politique et stratégie d'investissement

CANARIE continuera d'investir et de gérer les fonds qui lui sont avancés selon les politiques, les normes et les procédures que suivrait avec prudence une personne chargée de prendre des décisions sur l'investissement de biens qui ne lui appartiennent pas. CANARIE administrera les fonds conformément aux modalités de l'Accord de contribution, plus précisément les lignes directrices de son annexe E. L'objectif est double : a) procurer à l'organisation les fonds nécessaires au moment où elle en a besoin pour couvrir ses dépenses et b) optimiser les revenus de placement grâce à la stratégie et à la politique pertinentes adoptées par CANARIE.

La politique et la stratégie d'investissement en question précisent la nature des transactions permises et les risques maximaux tolérés dans les opérations commerciales et de crédit de l'organisme, de même que le pouvoir décisionnel des personnes autorisées à effectuer ces opérations pour le compte de l'organisation. La politique et la stratégie d'investissement sont révisées chaque année. Le Comité de la vérification comptable et des placements les a examinées en octobre 2025. La politique en matière de placements est régie par les exigences de l'Accord de contribution.

6. Stratégie de surveillance du rendement et stratégie d'évaluation et d'atténuation des risques

6.1 Surveillance du rendement

CANARIE recueille des données sur l'ensemble de ses programmes et services ainsi que sur son réseau à l'interne. On glane aussi des mesures externes du rendement dans la communauté, au moyen de sondages et de rapports, ainsi qu'avec le concours des réseaux régionaux. CANARIE collabore avec le ministre pour incorporer ces informations à une stratégie générale de gestion du rendement. Enfin, les données sur le rendement de chaque activité admissible sont exposées dans le rapport que CANARIE produit chaque année.

6.2 Risques relatifs à la prestation des programmes

Étant donné la diversité et la complexité de l'écosystème dans lequel il opère, CANARIE doit absolument gérer les risques pour atteindre les résultats souhaités, énoncés dans l'Accord de contribution. La direction de l'organisme signale les risques au conseil d'administration, qui en assure la surveillance.

Les risques sont classés d'après la probabilité qu'ils se concrétisent et la gravité de leurs conséquences. La façon dont ils sont traités varie en fonction de ces deux paramètres, comme l'indique le tableau ci-dessous.

		Probabilité		
		Faible	**Moyenne**	**Élevée**
Impact	**Faible**	Tolérer le risque	Tolérer le risque en le surveillant	Surveiller le risque et le gérer
	Modéré	Tolérer le risque en le surveillant	Élaborer des mesures d'atténuation	Dresser un plan pour atténuer le risque
	Élevé	Identifier des mesures d'atténuation et suivre la situation régulièrement	Prendre des mesures d'atténuation officielles et suivre la situation régulièrement	Dresser un plan d'atténuation officiel et suivre la situation régulièrement

Risque	Description	Prob.	Impact	Risque	Stratégie d'atténuation et plan d'action
Projet pilote de SOC fédéré du CanSSOC	CANARIE pourrait ne pas obtenir de fonds suffisants pour étendre et exploiter le SOC fédéré.	M	M	MM	• La demande de fonds soumise illustre clairement l'utilité et la faisabilité du SOC fédéré ainsi que la manière dont le projet s'accorde avec les objectifs d'ISDE, de CANARIE et de la collectivité que dessert l'organisation • Communications fréquentes avec ISDE et d'autres ministères sur la demande de financement
Intrusion IT dans l'organisme	Une intrusion dans les systèmes internes de CANARIE pourrait exposer des informations financières, contractuelles et personnelles, ce qui ternirait la réputation de l'organisation.	E	E	EE	• Investir constamment dans les TI • Appliquer les correctifs et améliorer les pratiques • Détecter les attaques par DDoS • Dispenser de la formation en sécurité, surveiller la situation • Dresser des plans d'intervention • Instaurer un programme d'audit en cybersécurité
Intrusion dans le réseau CANARIE	Une intrusion dans la dorsale du réseau pourrait exposer des données de recherche, ouvrir une porte qui mettrait en danger les institutions raccordées au réseau et ternir la réputation de l'organisation.	E	E	EE	• Investir dans les mesures de sécurité • Détecter les attaques par DDoS • Appliquer les normes de sécurité du MANRS afin de protéger le réseau • Suivre les directives du gouvernement canadien concernant les fournisseurs

Intrusion dans le RNRE	Une intrusion dans le réseau d'un partenaire du RNRE pourrait affecter le réseau CANARIE et ternir la réputation du RNRE, donc celle de l'organisation.	M	E	ME	• Investir conjointement dans la sécurité • Des analystes en sécurité ont été mis en place chez les partenaires du RNRE et collaborent à l'échelle nationale. • Cadre commun en cybersécurité • Créer un bulletin de note en sécurité pour le RNRE
Risque d'une guerre économique (droits de douane) entre le Canada et les États-Unis	La modification des droits de douane et les tarifs de rétorsion sur l'équipement essentiel au réseau pourraient empêcher CANARIE d'acheter du matériel ou de renouveler les ententes conclues avec les fournisseurs américains, ce qui nuirait à ses activités.	E	M	ME	• Étudier des stratégies pour remédier aux risques éventuels associés à la fluctuation des devises • Rester au courant de la situation économique et politique et déterminer comment réagir aux problèmes qui surviennent • Revoir les risques associés à la fluctuation des prix pour les ententes existantes et établir de nouveaux contrats qui exposeront moins l'organisation en négociant certaines conditions comme un plafonnement de la majoration des coûts, des mécanismes pour ajuster les prix, etc. • Examiner les ententes qui arrivent à terme et envisager des solutions de rechange longtemps avant leur renouvellement • Collaborer avec les fournisseurs