Partagé avec
TLP (Traffic Light Protocol) –
VERT

Approuvé

Norme en matière de sécurité physique des centres de données

ID du document : **SEC-01**

À l'attention de: Fédération de l'Alliance

Approuvé le 2024-10-01

Approuvé par le Conseil national de la sécurité (CNS)

1. Introduction

La cybersécurité est l'un des éléments fondamentaux qui assure l'efficacité des services fournis par la Fédération de l'Alliance. La présente politique et ses normes, procédures, spécifications et autres documents associés décrivent le cadre d'application des mesures la Fédération de l'Alliance.

2. Définitions

Pour l'ensemble des définitions, reportez-vous à SEC-00 Glossaire de la sécurité de l'information.

3. Applicabilité

La présente politique s'applique à tous les **Systèmes et services de la Fédération de l'Alliance**, aux données associées et à toute personne ayant accès à ces systèmes, services et données. Certains services sont dotés d'un modèle de responsabilité partagée, tel que défini dans leurs conditions particulières et dans certains cas, des responsabilités additionnelles sont attribuées à ses **Utilisatrices ou utilisateurs**.

4. Exigences en matière de cybersécurité

4.1 Protection des systèmes d'information

4.1.1 Tous les **Systèmes et services de la Fédération de l'Alliance**, ainsi que les données qui leur sont associées doivent être protégés d'une manière considérée comme étant raisonnable et appropriée à la classification et à la criticité des données, tout au long de leur cycle de vie.

4.1.2 La Fédération de l'Alliance doit implémenter des contrôles appropriés pour préserver la confidentialité, diponibilité et l'intégrité des données stockées et traitées au sein des **Systèmes et services de la Fédération de l'Alliance,** conformément au CRCFA.

4.1.3 L'accès aux **Systèmes et services de la Fédération de l'Alliance** et aux données qui leur sont associées doit être autorisé et limité sur la base du principe de privilège minimal.

4.1.4 Tout incident de sécurité suspecté ou confirmé touchant les **Systèmes et services de la Fédération de l'Alliance** doit être immédiatement signalé à security@tech.alliancecan.ca.

4.3 Formation et sensibilisation

- Toutes les Professionnelles ou professionnels de l'IRN de l'Alliance doivent suivre le ou les programmes de formation et de sensibilisation qui sont définis pour leur rôle dans le **Cadre de référence pour la cybersécurité de la Fédération de l'Alliance.**

4.4 Surveillance

Toute utilisation des **Systèmes et services de la Fédération de l'Alliance** doit être surveillée de manière vérifiable par audit, conformément au CRCFA.

4.5 Entente de service

La Fédération de l'Alliance doit documenter les exigences en cybersécurité du CRCFA dans une entente de service pour l'infrastructure et tous les services qu'elle offre (les exemples incluent les Conditions d'utilisation, l'Entente de niveau de service, le Protocole d'entente, l'Entente de contribution, etc.). Au minimum, l'accord de service doit inclure les détails et les rôles (RACI) pour les aspects suivants :

- Réponse aux incidents
- Accès à l'information
- Sauvegarde
- Maintenance
- Propriété des données
- Cycle de vie des données
- Journalisation et surveillance

4.6 Demande d'exception

Dans le cas où il est impossible de se conformer à un aspect quelconque du CRCFA, une demande d'exception peut être faite en écrivant à security@tech.alliancecan.ca. Toute demande d'exception doit être approuvée par la Vice-présidence des opérations et de la sécurité, à leur discrétion, et en consultation avec le Conseil consultatif et directeur sur la cybersécurité (CCDC), au besoin.

4.7 Rôles et responsabilités

La cybersécurité est une responsabilité qui incombe à tous et toutes : Utilisateurs et utilisatrices, **Professionnelles ou professionnels de l'IRN de l'Alliance** et personnel administratif. Toutes et tous doivent prendre les mesures nécessaires pour protéger les **Systèmes et services de la Fédération de l'Alliance** des cybermenaces potentielles. Ceci signifie qu'il faut se conformer à toutes les politiques, normes, procédures et spécifications de la Fédération de l'Alliance, d'être au courant des risques, d'implémenter des mesures de sécurité strictes et d'exercer une vigilance constante face à d'éventuelles attaques. En travaillant ensemble, nous pouvons créer un environnement de recherche numérique plus sûr et mieux sécurisé pour tous.

4.8 Gouvernance et documentation

La Vice-présidence des opérations et de la sécurité de l'Alliance est Imputable de veiller à ce qu'un programme de cybersécurité approprié, comprenant un cadre de politique et de gouvernance, soit établi, maintenu et publié pour la Fédération de l'Alliance. La Vice-présidence des opérations et de la sécurité de l'Alliance doit demander au Conseil national de sécurité (CNS) d'établir un groupe de travail chargé d'examiner et de maintenir ce cadre de politique et de gouvernance. Ceci comprend, sans toutefois s'y limiter :

- le programme et la stratégie pour la cybersécurité;
- la création, la maintenance et la révision périodique des documents du CRCFA, notamment :
    - les politiques, normes, procédures et spécifications;
- la création et la maintenance de documents de soutien, par exemple les directives et les listes de contrôle.

4.9 Implémentation

L'implémentation efficace du programme de cybersécurité concerne plusieurs groupes différents. La Vice-présidence des opérations et de la sécurité de l'Alliance est imputable d'assurer l'implémentation dans son ensemble. Différents aspects de l'implémentation du programme relèvent de la responsabilité de différents groupes (voir la matrice RACI dans la section 4.12 de ce document).
Les aspects de l'implémentation du programme incluent

- les investissements et ressources
- la gestion des projets du **Cadre de référence pour la cybersécurité de la Fédération de l'Alliance**
- la formation et la sensibilisation en lien avec le CRCFA
- la gestion du risque
- la gestion des incidents
- les opérations reliées à la sécurité, par exemple le renseignement sur les cybermenaces (*threat intelligence)*, la gestion des vulnérabilités, etc.)
- les demande d'exception et priorisation
- l'amélioration continue

4.10 Conformité et audits

Le Comité de gestion opérationnelle est imputable d'assurer que des audits de conformité du CRCFA et des audits pour l'ensemble de la Fédération de l'Alliance soient effectués ou de commandés. Le Comité de gestion opérationnelle doit travailler en collaboration avec l'OSAC, le

Centre des Opérations de Sécurité (COS) et le CNS de pour colliger les informations nécessaires, documenter les conclusions et communiquer les priorités des améliorations qui en résultent. Ces tâches comprennent, sans toutefois s'y limiter

- les audits opérationnels et le suivi (audits internes);
- les audits externes.

4.11 Rapports et métriques

Le rapport de métriques lié à la cybersécurité est requis afin d'évaluer l'efficacité du programme de cybersécurité, par les organismes responsables de la supervision de l'Alliance. La Vice-présidence des opérations et de la sécurité de l'Alliance est imputable de s'assurer à ce que la collecte des données nécessaires soit faite et adéquatement rapportée. Le CNS et le COS sont les principaux groupes responsables de la collecte des données. Les tâches sont :

- la collecte et identification des métriques;
- les rapports sur les opérations d'amélioration continue du CRCFA
- les rapports à l'intention de Innovation, Sciences et Développement économique Canada (ISDE);
- les rapports à l'intention des organisations partenaires.

4.12 Matrice RACI des activités reliées à la cybersécurité

	Gouvernance et documentation	Implémentation	Conformité et audits	Report et métriques
Vice-présidence des opérations et de la sécurité de l'Alliance	A	A	C	A
Comité de gestion opérationnelle	C	C	A	I
CCDC	C	C	I	I
CCDO	C	C	R	I
CNS	R	R	R	R

COS	C	R	R	R
Conseil de leadership technologique	C	R	I	I
Professionnelle ou professionnel de l'IRN de l'Alliance	C	R	-	-
Utilisateurs et utilisatrices	I	R	-	-

5. Information connexe

SEC-00 Glossaire de la cybersécurité
SECSD-00 Registre des documents de gouvernance