Politique de classification des données

ID du document: **SEC-02**
À l'attention de: Fédération de l'Alliance
Approuvé le 2022-03-15
Approuvé par le Conseil consultatif et directeur sur la cybersécurité (CCDC)

1. Introduction

La présente politique a pour objet d'établir la méthodologie de classification des données en fonction de leur niveau de sensibilité, de leur valeur et de leur criticité pour la Fédération, tel que requis par *SEC-05 Politique de gestion des risques liés à la cybersécurité*. La classification des données aidera à déterminer les contrôles de sécurité de base pour la protection des données en fonction du niveau de risque correspondant. Cette classification est importante pour s'assurer que les données bénéficient du niveau de protection approprié.

2. Définitions

Reportez-vous à *SEC-00 Glossaire de la sécurité de l'information* pour la définition des termes utilisés dans la présente politique.

3. Applicabilité

3.1 La présente politique s'applique à toutes les personnes ainsi qu'à tous les autres affiliés qui sont autorisés à accéder à un ou à plusieurs ***services nationaux*** et qui sont responsables de la classification et de la protection des données dans les systèmes de la Fédération de l'Alliance et de ses affiliés.

3.2 Rôles et responsabilités

3.2.1 L'intendante ou l'intendant des données/la ou le propriétaire des données est responsable d'établir la classification de sécurité de ses ensembles de données. Dans le cours de ses activités, la Fédération de l'Alliance peut traiter ou gérer les données comme si leur niveau de risque était supérieur au niveau déterminé, mais n'utilisera jamais un niveau inférieur. Par exemple, les données peuvent être classées à un niveau plus élevé que celui attribué dans le tableau 4.1, mais ne peuvent être reclassées à un niveau moins élevé.

3.2.2 La ou le gestionnaire des données doit connaître les types de données électroniques placées sous son contrôle; les risques potentiels liés aux ensembles de données dont elle ou il est responsable et qui peuvent toucher la Fédération de l'Alliance et ses affiliés; la classification de sécurité des données dont elle ou il est responsable; ainsi que l'emplacement où les données sont stockées.

4. Classification

4.1 Classification des données

La classification suivante décrit les niveaux de risques auxquels la Fédération ou ses affiliés seraient exposés dans un cas où la confidentialité, l'intégrité ou la disponibilité des données serait compromise. La classification reflète également la valeur inhérente des données et les contrôles qui doivent être mis en place pour les protéger.

Information de risque faible (niveau 1)

Exemples

- Informations ne nécessitant aucune protection.
- Informations accessibles au public (p. ex., rapports annuels publiés, communiqués de presse, articles de presse).
- Noms et coordonnées professionnelles des membres de l'équipe de la Fédération de l'Alliance.
- Informations susceptibles d'être publiées sur des sites Web publics.
- Informations de nature non personnelle et non exclusive, y compris des données de recherche anonymes lorsque l'accès à ces données n'est pas restreint.

Risques potentiels

- Gêne mineure, mais l'impact reste très limité.

Information de risque modéré (niveau 2)

Exemples

- Informations exclusives reçues d'un tiers en vertu d'accords de non-divulgation ou que nous partagerions en vertu d'accords de non-divulgation si les catégories à risque plus élevé ne s'appliquent pas.
- Périodiques à diffusion restreinte.
- Informations et rapports financiers agrégés.
- Informations techniques sur les systèmes ou les installations, qui ne sont pas susceptibles d'entraîner des dommages si elles sont dévoilées.
- Informations de nature non personnelle et non exclusive, y compris des données de

recherche anonymes lorsque l'accès à ces données devrait être restreint.

Risques potentiels

- Impact limité sur la réputation ou les finances d'un site hôte national ou d'un affilié.
- Impact limité sur les activités d'un site hôte national ou d'un affilié.
- Perte de priorité de publication (p. ex., nous ne serions plus les premiers à publier).
- Perte d'accès à des périodiques ou à d'autres documents protégés par droit d'auteur.

Risque élevé (niveau 3)

Exemples

- Données contrôlées nécessitant une protection par la loi, par un accord de non-divulgation ou par la réglementation de l'industrie.
- Données associées à des brevets ou à des demandes de brevet.
- Informations permettant d'identifier une personne.
- Informations et dossiers financiers confidentiels.
- Informations techniques qui facilitent la compromission des systèmes ou des installations.
- Données de recherche dont la collecte ou la reproduction nécessiterait des efforts ou des coûts importants (p. ex., du financement supplémentaire pourrait être nécessaire).

Risques potentiels

- Impact sur la réputation ou les finances d'un site hôte national ou d'un affilié.
- Impact sur les activités d'un site hôte national ou d'un affilié.
- Potentiel d'usurpation d'identité.
- Potentiel de fraude ou de harponnage.

Risque très élevé (niveau 4)

Exemples

- Informations d'une carte de paiement d'un client lorsqu'un site hôte national ou un affilié agit en qualité de commerçant.
- Renseignements personnels sur la santé, tels que définis par la législation provinciale ou fédérale.
- Données génétiques permettant d'identifier une personne.
- Données biométriques.
- Copie d'une carte d'identité du gouvernement.
- Logiciel ou ensemble de données de recherche de nature stratégique ou sensible.
- Données permettant d'identifier une personne et protégées par la réglementation/législation (p. ex., le *Règlement général sur la protection des données*, ou RGPD).
- Données de recherche qu'il peut être impossible de collecter ou de reproduire.

Risques potentiels

- Impact sérieux sur la réputation ou les finances de plusieurs sites hôtes nationaux ou d'affiliés.
- Impact sérieux sur les activités de plusieurs sites hôtes nationaux ou d'affiliés.
- Pertes financières (amendes réglementaires ou dommages-intérêts résultant d'un litige).
- Perte de compétitivité dans un domaine de recherche stratégique clé.
- Usurpation d'identité qui affecte gravement les personnes concernées.

5. Directive

5.1 Norme de gestion des données

Le Conseil national de sécurité doit publier et maintenir une norme relative à la gestion des données qui spécifie les exigences de traitement et de contrôle pour chacune des classifications de données répertoriées dans la présente politique.

6. Information connexe

SEC-00 Glossaire de la sécurité de l'information
SEC-05 Politique de gestion des risques liés à la cybersécurité
SEC-03 Norme de gestion des données