Norme de gestion des données

ID du document: **SEC-03**

À l'attention de: Fédération de l'Alliance

Approuvé le 2022-08-24

Approuvé par le Conseil national de la sécurité (CNS)

1. Introduction

La présente norme décrit en détail le traitement approprié des données en fonction de leurs classifications définies dans *SEC-02 Politique de classification des données*.

2. Définitions

Reportez-vous à *SEC-00 Glossaire de la sécurité de l'information*.

3. Applicabilité

La présente norme s'applique aux données stockées, traitées et transmises par la Fédération de l'Alliance.

4. Exigences en matière de traitement des données

4.1 Étiquetage des données/avis de non-responsabilité

Dans la mesure du possible, les données à risque modéré, élevé ou très élevé doivent être étiquetées pour indiquer leur classification et leur propriétaire, conformément à *SEC-02 Politique de classification des données*. La méthode d'étiquetage des données dépendra de leur format. Ainsi, l'étiquetage peut prendre les formes suivantes :

- En-tête/pied de page du document
- Métadonnées liées ou intégrées
- Avis de non-responsabilité ou fichier Lisez-moi pour décrire une collection ou un ensemble de données
- Message en bannière dans l'application/la base de données
- Couverture imprimée pour copie papier ou autre support physique

De préférence, les étiquettes doivent être visibles lors de l'accès direct aux données (p. ex., dans le document plutôt que dans un fichier Lisez-moi).

4.2 Inventaire des données

La ou le propriétaire des données ou l'intendant(e) des données désigné(e) doit tenir un inventaire de toutes les données à risque élevé ou très élevé sous sa responsabilité. Au minimum, l'inventaire doit contenir les éléments suivants :

- Propriétaire des données
- Intendant(e) des données, s'il y a lieu
- Classification des données
- Emplacement/système
- Média/format (document numérique, base de données, copie papier)
- Une description générale

4.3 Données détenues par des tiers

Les données de la Fédération de l'Alliance gérées par des tiers, y compris les fournisseurs et les partenaires, doivent être traitées conformément à la présente norme. En outre, la *Liste de contrôle de sécurité du fournisseur* doit être remplie avant de fournir l'accès aux données de la Fédération de l'Alliance.

4.4 Renforcement des systèmes et des services

Les systèmes, les services et leur infrastructure sous-jacente doivent être renforcés conformément aux meilleures pratiques de l'industrie, notamment à l'aide de :

- l'utilisation d'un système de gestion des configurations;
- la désactivation des services inutiles;
- l'exposition limitée au réseau et aux comptes d'accès;
- l'isolement des ressources.

4.5 Transmission des données

Par transmission des données, on entend le déplacement d'une copie des données d'un endroit à un autre. Lorsque des données sont transférées d'un domaine de sécurité à un autre, elles doivent être sécurisées conformément à leur classification.
Toutes les données doivent être transférées conformément aux meilleures pratiques de l'industrie en vue du chiffrement en transit (voir https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062).
Il est recommandé que toutes les données soient transférées via un canal chiffré, dans la mesure du possible.

Le tableau suivant présente des exemples de modalités de partage/transmission de données basées sur la classification :

Exemple	**Risque faible**	**Risque modéré**	**Risque élevé**	**Risque très élevé**
Courriel[1]	Acceptable	Acceptable	Non recommandé : utiliser une pièce jointe chiffrée, au besoin.	
Courriel (personnel/autre)	Acceptable	Non recommandé	Interdit	
Globus	Recommandé (quand les transferts chiffrés sont utilisés)			
Outils de collaboration[2] (OTRS, Gitlab)	Recommandé	Non recommandé	Interdit	
Clavardage; Slack[2]	Recommandé		Acceptable	Interdit
Outils de visioconférence (Slack[2], Meet[2], Zoom[1], Teams[1])	Recommandé			
Partage de fichiers (G-Suite[2], NextCloud[2])	Recommandé			
Outils de tiers (Dropbox, comptes personnels, autres outils d'un établissement, etc.)	Non recommandé	Interdit		

4.6 Protection au repos

Les données doivent être stockées, consultées et conservées conformément aux meilleures pratiques de l'industrie, y compris le chiffrement au repos. La technologie de chiffrement choisie doit garantir des niveaux de confidentialité appropriés contre l'accès de tiers non autorisés. Des exemples de méthodes de chiffrement acceptables incluent le chiffrement complet du disque,

[1] Tenant de l'Alliance de recherche numérique du Canada
[2] Tenant de la Fédération de l'Alliance

du volume et du fichier. Le tableau suivant présente des exemples de cas et indique si l'utilisation du chiffrement est facultative, recommandée ou obligatoire :

Emplacement de stockage	Risque faible	Risque modéré	Risque élevé	Risque très élevé
Centres de données de la Fédération de l'Alliance	Facultatif	Recommandé	Obligatoire	Obligatoire
Nuages du commerce	Facultatif	Recommandé	Obligatoire	Obligatoire
Établissements partenaires	Facultatif	Recommandé	Obligatoire	Obligatoire
Ordinateurs portatifs et autres périphériques (p. ex., clé USB à minidisque dur, clé USB, téléphone intelligent)	Facultatif	Obligatoire	Obligatoire	Obligatoire
Toutes les autres données	Facultatif	Obligatoire	Obligatoire	Obligatoire

4.7 Audit et journalisation

L'accès à toutes les données doit être enregistré conformément à *SEC-05 Norme de journalisation des systèmes et de surveillance de la sécurité*.

4.8 Sauvegarde et restauration

La classification des données doit être prise en compte dans le cadre du processus de sauvegarde et de restauration. Les mêmes contrôles et principes doivent être appliqués aux données à toutes les étapes du cycle de vie et à toutes les copies de données (p. ex., stockage portable, emplacements de stockage temporaire, espace de travail).

4.9 Gestion des correctifs

Des correctifs doivent être ajoutés régulièrement à tous les actifs de la Fédération de l'Alliance. Avant l'application des correctifs aux environnements de production, les modifications doivent être testées dans un environnement de non-production pour s'assurer de l'absence d'impacts négatifs.

4.10 Gestion des vulnérabilités

Les systèmes, les services et leur infrastructure sous-jacente doivent faire l'objet d'une analyse régulière des vulnérabilités conformément à *SEC-04 Norme de gestion des vulnérabilités*.

4.11 Points d'extrémité et sécurité physique

Le traitement des données, ce qui comprend le personnel concerné par le traitement des données, doit être protégé conformément aux normes de l'industrie, notamment par :

- l'imposition de délais d'inactivité pour les écrans;
- l'utilisation d'appareils non partagés;
- le déverrouillage nécessaire pour accéder aux systèmes et aux services;
- la mise à jour automatique des logiciels et des correctifs;
- l'utilisation d'antivirus ou de la technologie EDR (Endpoint Detection and Response);
- des mesures raisonnables de sécurité des réseaux (voir https://www.getcybersafe.gc.ca/fr);
- la sensibilisation à l'environnement et à l'espionnage par-dessus l'épaule;
- la sensibilisation à l'ingénierie sociale et aux attaques d'hameçonnage.

4.12 Élimination/destruction des données

Toutes les données doivent être conservées aussi longtemps que l'exigent la réglementation et/ou la politique applicable. Une fois que les données ne sont plus nécessaires, elles doivent être détruites, y compris dans les cas de réutilisation des dispositifs de stockage.
Consultez https://cyber.gc.ca/fr/orientation/nettoyage-et-elimination-dappareils-electroniques-its ap40006 pour plus d'information (notez que l'effacement et la réinitialisation aux paramètres d'usine est une mesure insuffisante pour détruire des données).

Le tableau suivant résume les méthodes appropriées à employer :

Méthode	Support magnétique chiffré	Support magnétique non chiffré	Dispositif à semi-conducteurs chiffré	Dispositif à semi-conducteurs non chiffré
Écrasement et effacement sécurisé	✓	✓		
Effacement cryptographique	✓		✓	
Démagnétisation	✓	✓		
Destruction physique	✓	✓	✓	✓

- Inclut les appareils mobiles et appareils pour l'Internet des objets.
- Lors de la suppression de données d'un système de stockage actif, toutes les copies de sauvegarde des données doivent également être supprimées et purgées dès que possible, au plus tard après 12 mois.
- Les données détenues par les fournisseurs doivent être certifiées comme étant détruites par l'un des moyens spécifiés dans la *Liste de contrôle de sécurité des fournisseurs*.

5. Information connexe

SEC-00 Glossaire de la sécurité de l'information
SEC-02 Politique de classification des données
SEC-04 Norme de gestion des vulnérabilités
SEC-06 Norme de journalisation des systèmes et de suivi de la sécurité
Liste de contrôle de sécurité des fournisseurs