Titre:	**Exigences minimales de sécurité liées à la sauvegarde des données**		
État :	Approuvé	Approbation :	2023-09-13
		Mise à jour :	2023-11-06

Type :	Exigences		
Code du document :	MSSS-EXI-007	Portée :	MSSS et RSSS
Mots clés :	Exigences minimales; Sauvegarde; Plan de reprise; Contrôle d'accès; Infrastructure; Chiffrement; Résilience; Tests		
Justification :	Le RSSS et le MSSS offrent des services qui s'appuient fortement sur les technologies de l'information (TI). De ce fait, l'un des outils fondamentaux de la continuité de ces services est le plan de reprise informatique (PRI), qui s'avère également une mesure d'atténuation des risques liés à la sécurité de l'information. Des copies de sauvegardes récentes, intègres et disponibles à l'intérieur d'un délai acceptable pour l'organisation sont la pierre angulaire de la qualité d'un PRI. **Précisions complémentaires** Le présent document regroupe les mesures de sécurité obligatoires relatives à la sauvegarde des données. Ces mesures doivent être appliquées à l'ensemble des systèmes de sauvegarde des données appartenant au MSSS ainsi qu'au RSSS et gérées par l'une des équipes des technologies de l'information de ces organisations.		

Déclaration :	**Contrôler l'accès aux systèmes de sauvegarde**
Précisions :	
Il s'agit d'appliquer un contrôle d'accès strict sur le système de sauvegarde de manière à limiter les risques de compromissions. Cela peut être fait en : • Créant des comptes administrateurs dédiés; • Mettant en place des mécanismes d'authentification forts tels que les jetons d'authentification, les codes à usage unique ou autres méthodes disponibles permettant de renforcer la sécurité de ces comptes d'administration; • Journalisant tous les accès et les événements de sécurité liée à ces comptes; • Révisant sur une base régulière les permissions accordées à ces comptes. Ces comptes ne doivent pas être utilisés en dehors des activités liées à la sauvegarde afin d'éviter de laisser des traces en dehors du système de sauvegarde. Il s'agit également d'appliquer les principes du « **moindre privilège** », du « **besoin de savoir** » et de « **séparation des responsabilités (ou des tâches)** » afin de n'accorder que les privilèges nécessaires aux personnes ayant accès au système de sauvegarde.	
Justification :	Réduire le risque d'exposition des données de sauvegarde et se prémunir contre les attaques basées sur la compromission de l'identifiant d'un administrateur.

Lien avec :	Extranet du MSSS, section Sécurité de l'information :
	(https://extranet.ti.msss.rtss.qc.ca/Securite-de-l-information/Gouvernance.aspx)
	• Directive sur l'élaboration et l'évolution d'un plan de reprise informatique - MSSS-DIR11
	• Mesures minimales - Ministère de la Cybersécurité et du Numérique
	  ○ Présentation des 15 mesures
	  ○ Actions et spécifications pour chaque mesure

Déclaration :	**Isoler l'infrastructure de sauvegarde**
Précisions :	
Il s'agit d'isoler l'infrastructure de sauvegarde dans un réseau distinct et de mettre en place des règles de sécurité réseau stricte qui limitent l'accès aux personnes et aux systèmes préalablement autorisés. Cela peut être fait en utilisant les principes de microsegmentation pour protéger cette infrastructure. Il s'agit également de mettre en place un processus permettant de « débrancher » l'infrastructure de sauvegarde dès qu'une attaque par rançongiciel est détectée afin de protéger cette infrastructure.	
Justification :	• Minimiser les risques de pertes de données; • Maintenir la continuité des opérations en améliorant la fiabilité du système de sauvegarde; • Protéger l'intégrité des données constituant les copies de sauvegarde; • Prévenir la propagation des attaques par rançongiciel.

Lien avec :	Extranet du MSSS, section Sécurité de l'information :
	(https://extranet.ti.msss.rtss.qc.ca/Securite-de-l-information/Gouvernance.aspx)
	• Directive sur l'élaboration et l'évolution d'un plan de reprise informatique - MSSS-DIR11
	• Mesures minimales - Ministère de la Cybersécurité et du Numérique
	  ○ Présentation des 15 mesures
	  ○ Actions et spécifications pour chaque mesure
	Et :
	• Guide sur les rançongiciels du Centre canadien pour la cybersécurité (https://www.cyber.gc.ca/sites/default/files/cyber/2021-12/itsm00099-guide-rancongiciels-2021-final4-fr.pdf)

Déclaration :	**Chiffrer les copies de sauvegarde des données**
Précisions :	
Cette mesure s'applique à la transmission des données de sauvegarde ainsi qu'aux supports de stockage de ces données, tant sur des médias conventionnels que dans l'infonuagique. Il s'agit de chiffrer ces copies dans leur intégralité, aussi bien en transit qu'au repos, y compris les métadonnées qui leur sont associées, afin de garantir la confidentialité de ces données. Des algorithmes de chiffrement symétrique des données reconnus et robustes doivent être utilisés, Advanced Encryptions Standard (AES) 256 bits par exemple. Des pratiques de gestion rigoureuses des clés sécurisées doivent être mises de l'avant, par exemple : • la limitation de l'accès à ces clés uniquement aux personnes autorisées; • la sauvegarde sécurisée de ces clés; • la mise en place de mécanismes de récupération en cas de perte ou d'indisponibilité de ces clés; • le remplacement des clés compromises.	
Justification :	Le préjudice associé à la divulgation des données de sauvegarde est le même que celui des données elles-mêmes. Le niveau de sécurité doit conséquemment être au moins équivalent à celui des données de production les plus sensibles contenues dans ces sauvegardes. Le chiffrement des sauvegardes permet de protéger et d'empêcher les accès non autorisés aux données sensibles de l'organisation.

Lien avec :	Extranet du MSSS, section Sécurité de l'information :
	
	(https://extranet.ti.msss.rtss.qc.ca/Securite-de-l-information/Gouvernance.aspx)
	
	• Directive sur l'élaboration et l'évolution d'un plan de reprise informatique - MSSS-DIR11
	• Mesures minimales - Ministère de la Cybersécurité et du Numérique
	  ○ Présentation des 15 mesures
	  ○ Actions et spécifications pour chaque mesure
	
	Et :
	
	Sauvegarde et chiffrement des données du Centre canadien pour la cybersécurité (https://www.cyber.gc.ca/fr/orientation/sauvegarde-et-chiffrement-des-donnees)

Déclaration :	**Vérificer l'intégrité des données sauvegardées**
Précisions :	
Il s'agit d'adopter une procédure de vérification systématique de l'intégrité des données sauvegardées : • en comparant le hachage des données avec le hachage des données originales; • en vérifiant la validité des signatures dans le cas où les données sauvegardées sont signées numériquement. Cette vérification doit être effectuée après chaque sauvegarde. Une mesure corrective automatique ou manuelle doit être prise dès qu'un problème d'intégrité est détecté à la suite de cette vérification.	
Justification :	Détecter rapidement toute altération qui pourrait compromettre l'intégrité des données sauvegardées et ainsi rendre la sauvegarde inutilisable en cas de sinistre ou de cyberattaque.

Lien avec :	Extranet du MSSS, section Sécurité de l'information :
	(https://extranet.ti.msss.rtss.qc.ca/Securite-de-l-information/Gouvernance.aspx)
	• Directive sur l'élaboration et l'évolution d'un plan de reprise informatique - MSSS-DIR11
	• Mesures minimales - Ministère de la Cybersécurité et du Numérique
	  ○ Présentation des 15 mesures
	  ○ Actions et spécifications pour chaque mesure

Déclaration :	**Assurer la résilience des données de sauvegarde**
Précisions :	
Il s'agit d'appliquer la stratégie de sauvegarde 3-2-1 qui permet d'augmenter le nombre de copies et de diversifier les lieux où elles sont stockées. Cette stratégie assure la résilience des données par une redondance fiable et suit les règles suivantes : Stratégie 3 : Conserver trois copies des données, soit les données originales et deux copies supplémentaires. Stratégie 2 : Stocker ces trois copies sur deux types de supports différents. Stratégie 1 : S'assurer qu'au moins une des deux copies supplémentaires se trouve hors site et sous forme immuable (dont l'intégrité est protégée contre les modifications).	
Justification :	• Se protéger contre la perte et la corruption des données; • Réduire les risques de perte totale des données en raison de défaillances matérielles, d'erreurs humaines, d'attaques malveillantes ou de catastrophes naturelles.

Lien avec :	Extranet du MSSS, section Sécurité de l'information :
	(https://extranet.ti.msss.rtss.qc.ca/Securite-de-l-information/Gouvernance.aspx)
	• Directive sur l'élaboration et l'évolution d'un plan de reprise informatique - MSSS-DIR11
	• Mesures minimales - Ministère de la Cybersécurité et du Numérique
	  ○ Présentation des 15 mesures
	  ○ Actions et spécifications pour chaque mesure
	Et :
	• Guide sur les rançongiciels du Centre canadien pour la cybersécurité (https://www.cyber.gc.ca/sites/default/files/cyber/2021-12/itsm00099-guide-rancongiciels-2021-final4-fr.pdf)

Déclaration :	**Tester périodiquement la restauration des données**
Précisions :	
Il s'agit de mettre en place un processus de vérification du système de sauvegarde en effectuant des tests de restauration à une fréquence minimale d'au moins une fois par mois. Cette mesure vise à détecter, et à corriger, à l'avance, tout problème technique qui pourrait survenir dans le bon fonctionnement des procédures de restauration ou d'exécution de plan de reprise informatique. Il n'est pas nécessaire de restaurer un système complet, mais simplement de vérifier qu'il serait possible de le faire, le cas échéant, en procédant avec un échantillon. Ces tests doivent inclure des données stockées hors site.	
Justification :	S'assurer que la restauration des copies de sauvegarde est fonctionnelle.

Lien avec :	Extranet du MSSS, section Sécurité de l'information :
	
	(https://extranet.ti.msss.rtss.qc.ca/Securite-de-l-information/Gouvernance.aspx)
	
	• Directive sur l'élaboration et l'évolution d'un plan de reprise informatique - MSSS-DIR11
	• Mesures minimales - Ministère de la Cybersécurité et du Numérique
	  ○ Présentation des 15 mesures
	  ○ Actions et spécifications pour chaque mesure

Déclaration :	**Protéger les données des médias de stockage obsolètes**
Précisions :	
Cette exigence consiste principalement à anticiper l'usure des médias de sauvegarde, qui ont une durée de vie limitée, en migrant les données vers de nouveaux médias avant la fin de vie utile de ces médias. Une fois la migration effectuée, on doit s'assurer d'effacer, de manière permanente et non recouvrable, les données de sauvegarde emmagasinées sur les anciens médias de sauvegarde afin que ces données ne soient plus recouvrables. Pour ce faire, la destruction adéquate de ces médias est recommandée.	
Justification :	Se protéger contre le vol des données sensibles contenues sur les médias de sauvegarde et la perte d'information par suite d'une incapacité à récupérer les données d'un média défectueux.
Lien avec :	• Procédure de destruction de la Commission d'accès à l'information du Québec (https://www.cai.gouv.qc.ca/organismes/procedure-de-destruction/)

Déclaration :	**Surveiller les processus de sauvegarde**
Précisions :	
Les processus qui entourent la sauvegarde doivent être surveillés afin de s'assurer qu'ils se déroulent correctement et ce, plus particulièrement ceux touchant les actifs informationnels évalués comme étant critiques à l'organisation. De façon plus précise : • surveiller l'environnement de sauvegarde pour s'assurer - de manière centralisée – que toutes les composantes de l'outil de sauvegarde soient adéquatement configurées et conformes à la stratégie de sauvegarde préalablement établie par l'organisation; • s'assurer que les opérations de sauvegarde (suppression, rétention des modifications, mises à jour de la configuration de sauvegarde, etc.) soient surveillées, auditées et disposent d'alertes en place; • surveiller l'intégrité globale des copies de sauvegardes, configurer et recevoir des alertes en cas d'incidents afin d'intercepter et de traiter les évènements liés à l'intégrité des opérations de sauvegarde; • auditer les actions des utilisateurs disposant de privilèges d'accès aux sauvegardes.	
Justification :	Contrôler la bonne application de la stratégie de sauvegarde à travers la surveillance centralisée des sauvegardes pour minimiser le risque de perte de confidentialité, d'intégrité ou de disponibilité des données sauvegardées.