culture
Saguenay–Lac-Saint-Jean

GESTION DES ACCÈS ET DES PRIVILÈGES

Le verrou de votre sécurité numérique

(principe du moindre privilège)

OBJECTIF

Ce guide a pour objectif de vous accompagner dans la mise en œuvre du principe du moindre privilège au sein de votre organisation culturelle.

L'idée est simple : limiter les accès aux ressources numériques au strict nécessaire pour chaque utilisateur. En verrouillant ainsi vos systèmes, vous réduisez considérablement les risques de cyberattaques, les erreurs humaines involontaires et les abus de droits.

DÉFINITIONS ESSENTIELLES

TERMES	CONCEPTS	EXEMPLES
RBAC Role-Based Access Control	Donner les bonnes clés, selon le rôle	*Dans un musée, le/la médiateur·rice culturel·le a accès aux contenus éducatifs et au calendrier des visites, mais pas au système de paie ni aux contrats d'acquisition des œuvres.*
IAM Identity & Access Management	Un tableau de contrôle centralisé qui remplace le trousseau de clés chaotique. Chaque personne a une identité numérique unique, contrôlée et traçable.	*Un théâtre utilise une plateforme centrale pour gérer les accès : billetterie, site web, outils de création, courriels. Chaque employé·e a un seul profil, ajusté selon son rôle.*
JIT Accès juste-à-temps	Une clé temporaire pour une pièce sensible. Elle fonctionne seulement le temps nécessaire, puis disparaît automatiquement.	*Lors d'une exposition temporaire, un technicien externe reçoit un accès limité et temporaire au système de contrôle ou aux plans numériques, uniquement pour la durée du montage.*
MFA Authentification multifactorielle	Une double serrure : même si le mot de passe est volé, un second élément (cellulaire, application, code) bloque l'accès.	*Le/la responsable des collections doit confirmer son identité avec son téléphone en plus du mot de passe pour accéder à la base de données des œuvres et de leur valeur.*

RISQUES EN CAS DE MAUVAISE GESTION

→ **Atteinte à l'intégrité des métadonnées et à la rémunération**
Une modification non autorisée de vos identifiants permanents (comme le code ISRC ou ISNI) peut rendre vos œuvres invisibles et bloquer la redistribution de vos droits par la SOCAN.

→ **Altération ou suppression de données critiques**
Perte irrémédiable de documents d'archives historiques (fonds ISAD(G)) par une simple erreur de manipulation.

→ **Accès non autorisé aux données sensibles**
Fuite de contrats d'artistes, de fichiers de donateurs ou de métadonnées administratives confidentielles.

→ **Non-conformité réglementaire**
Risque de sanctions juridiques pour non-respect de la protection des données personnelles.

→ **Propagation rapide d'une cyberattaque**
Si un compte d'employé possède trop de droits, un ransomware peut chiffrer l'intégralité de vos collections numériques et de vos serveurs en quelques minutes

Ce document a été réalisé par Culture Saguenay–Lac-Saint-Jean.

culture
Saguenay–Lac-Saint-Jean

LES BONNES PRATIQUES À ADOPTER

- **Appliquer le strict nécessaire**
  N'accordez que les droits indispensables à l'exécution d'une tâche précise, ni plus, ni moins.
- **Séparer les usages**
  Utilisez des comptes distincts pour les tâches administratives (installation de logiciels) et les tâches courantes (courriels, navigation).
- **Réagir aux départs**
  Révoquez systématiquement et immédiatement tous les accès dès qu'un employé ou un stagiaire quitte l'organisation.
- **Généraliser le MFA**
  Activez l'authentification multifactorielle sur tous les comptes, en priorité pour ceux ayant accès à vos actifs numériques de valeur.
- **Auditer régulièrement**
  Prévoyez une révision périodique pour vérifier que chaque collaborateur possède toujours les accès appropriés à son poste.

À ÉVITER (LES DRAPEAUX ROUGES)

- X **Accorder des droits administrateurs par défaut**
  Tout le monde n'a pas besoin de pouvoir tout modifier ou tout supprimer.
- X **Donner des accès permanents sans justification**
  Les accès "à vie" pour des dossiers sensibles ne devraient jamais être la norme.
- X **Laisser des comptes "orphelins"**
  Les comptes d'anciens collaborateurs sont des portes d'entrée privilégiées pour les pirates.
- X **Partager des comptes**
  L'utilisation d'un identifiant unique pour plusieurs bénévoles ou employés empêche de savoir qui a fait quoi.
- X **Accumuler les privilèges (privilege creep)**
  Un employé change de département mais garde les accès de son ancien poste.

ASTUCE CLÉ

Si un accès n'est pas strictement nécessaire, il ne doit pas être accordé.

MESURES CONCRÈTES À METTRE EN PLACE

- ☐ **Mettre en œuvre une solution IAM :** Centralisez la gestion des identités pour ne plus perdre le contrôle.
- ☐ **Définir des profils d'accès par domaine :** Standardisez les droits selon les besoins métier (ex: profil "Archives" pour le standard ISAD(G), profil "Musique" pour la gestion des codes ISRC, profil "Arts Visuels" pour VRA Core).
- ☐ **Journaliser et surveiller :** Gardez une trace (logs) des accès aux fichiers sensibles pour détecter les comportements inhabituels.
- ☐ **Automatiser les processus :** Simplifiez l'attribution et le retrait des droits pour limiter l'oubli humain.
- ☐ **Planifier des revues d'accès :** Fixez une rencontre trimestrielle avec les responsables de départements pour valider les accès de leurs équipes.