POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Adoptée par le conseil d'administration par résolution n°1605, le 19 mars 2026

MAC

SOMMAIRE

Historique des modifications :	La *Politique de sécurité de l'information* (« Politique ») constitue la première version de ce document normatif adopté par le Musée d'art contemporain de Montréal (« MAC » ou « Musée »). Elle a été élaborée afin d'établir un cadre structuré pour la gouvernance et la protection des actifs informationnels, conformément aux exigences légales du Québec ainsi qu'aux directives et orientations émises par le Secrétariat du Conseil du trésor et le ministère de la Cybersécurité et du Numérique.
Recommandation pour adoption :	Le comité d'audit du conseil d'administration (« CA »), le 10 mars 2026.
Adoption par :	Le CA, le 19 mars 2026, résolution 1605.
Responsables :	La Direction des technologies est responsable de l'élaboration et de l'actualisation de la Politique, appuyé de la personne nommée cheffe de la sécurité de l'information organisationnelle (« CSIO »).
Champ d'application :	La Politique s'applique à toutes les personnes qui accèdent, utilisent, traitent ou gèrent de l'information ou des systèmes d'information du MAC, y compris les employées et employés, les cadres, les membres du CA, de ses comités et de ses sous-comités, les prestataires de services ainsi que les autres personnes tierces autorisées. La Politique s'étend aussi aux membres du personnel et aux personnes tierces associées à la Fondation du MAC. Elle couvre l'ensemble des actifs informationnels, quel que soit leur support, qu'il soit papier, numérique, audiovisuel ou autre, ainsi que leur environnement de traitement.
Gouvernance :	La Direction des technologies assure une reddition auprès de la direction générale, du comité de direction puis auprès du comité d'audit du CA, selon ses besoins, au sujet des activités liées à la Politique.
Contexte financier :	Les initiatives liées à la sécurité de l'information sont financées à même les budgets de fonctionnement du Musée.
Documents liés à l'application de la Politique :	• *Politique d'accès aux documents et de protection des renseignements personnels* • *Politique de gestion de l'information* • *Politique de gestion intégrée des risques* • *Code d'éthique et de déontologie du personnel du MAC.* • *Directive sur la gestion des incidents de sécurité de l'information* • *Directive sur la gestion des identités et des accès* • *Directive sur l'utilisation des ressources numériques, des appareils mobiles et services infonuagiques* • *Directive sur la gestion des équipements, des systèmes et des actifs technologiques* • *Directive sur les achats de biens et de services et de conduite en matière de gestion contractuelle* • *Registre de classification de sécurité* • *Inventaire des renseignements personnels* • *Inventaire des documents essentiels*

Cadre juridique :	• *Charte des droits et libertés de la personne* (RLRQ, c. C-12) • *Code civil du Québec* (RLRQ, c. CCQ-1991) • *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1) • *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1), telle que modifiée par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Loi 25, LQ 2021, c. 25) • *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (RLRQ, c. A-2.1, r. 2) • *Règlement sur les incidents de confidentialité* (RLRQ, c. A-2.1, r. 3.1) • *Loi sur les archives* (RLRQ, c. A-21.1) • *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques* (RLRQ, c. A-21.1, r. 2) • *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03) • *Loi sur les contrats des organismes publics* (RLRQ, c. C-65.1) • *Loi sur le droit d'auteur* (LRC 1985, c. C-42) • *Politique gouvernementale de cybersécurité* (mars 2020) • *Directive gouvernementale sur la sécurité de l'information* (décret no 1514-2021 du 8 décembre 2021) • *Modèle de classification de sécurité des données numériques gouvernementales* (arrêté ministériel numéro 2024-05)

1. PRÉAMBULE

La sécurité de l'information constitue un enjeu stratégique pour le MAC, qui s'engage à protéger la confidentialité, l'intégrité et la disponibilité de ses actifs informationnels. La *Politique de la sécurité de l'information* (« Politique ») vise à établir les principes et les responsabilités nécessaires pour assurer une gestion sécuritaire des informations et des systèmes qui les supportent, en conformité avec les lois, règlements et meilleures pratiques applicables. Elle s'inscrit dans une démarche proactive visant à prévenir les risques, à maintenir la confiance des parties prenantes et à soutenir la mission du Musée dans un environnement numérique en constante évolution.

2. OBJET

La Politique vise à établir le cadre de gouvernance, les principes directeurs et les responsabilités permettant d'assurer la protection de l'information et des systèmes d'information du MAC, tout au long de leur cycle de vie. Elle a pour objectif de garantir :

- La confidentialité de l'information ;
- L'intégrité des données et des systèmes ;
- La disponibilité de l'information nécessaire à la réalisation de la mission du Musée.

3. PRINCIPES DIRECTEURS

La sécurité de l'information repose sur les principes suivants :

a) **Confidentialité et contrôle des accès :** L'accès à l'information et aux systèmes est attribué uniquement par des personnes autorisées, selon les principes du besoin de connaître et du

moindre privilège, en lien avec les rôles et responsabilités. La divulgation est limitée aux personnes autorisées afin d'assurer la confidentialité des actifs informationnels.

b) **Intégrité des informations et des systèmes :** Garantir l'exactitude, la fiabilité et la cohérence des données et des systèmes d'information tout au long de leur cycle de vie.
c) **Proportionnalité des mesures de sécurité** : Adapter les contrôles de sécurité à la sensibilité, à la valeur et aux risques associés à l'information et aux activités.
d) **Prévention et gestion continue des risques** : Identifier, évaluer et traiter de façon continue les risques informationnels. Mettre en place des mesures proactives et maintenir un haut niveau de vigilance pour prévenir les incidents.
e) **Conformité légale et normative**: Respecter les lois, règlements et obligations applicables, notamment en matière de protection des renseignements personnels, ainsi que les politiques et normes internes.
f) **Responsabilisation et sensibilisation du personnel**: La sécurité de l'information est une responsabilité partagée. Chaque personne protège l'information qu'elle crée, utilise ou à laquelle elle a accès et adopte les meilleures pratiques grâce à des activités de sensibilisation et de formation.
g) **Encadrement contractuel des tierces parties :** Les contrats et ententes avec des personnes utilisatrices ou intervenantes externes (ex. : prestataires, consultantes ou consultants, etc.) incluent des dispositions assurant le respect de la Politique et des exigences de sécurité.
h) **Gouvernance et collaboration avec les parties prenantes :** La gouvernance de la sécurité de l'information collabore de façon continue avec l'ensemble des parties prenantes, afin de renforcer la sécurité, réduire les risques, promouvoir la conformité et assurer une communication ouverte et transparente.
i) **Éthique :** Le processus de gestion de la sécurité de l'information doit être soutenu par une démarche éthique visant à assurer la régulation des conduites et la responsabilité individuelle.
j) **Évolution :** Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être réévaluées périodiquement et actualisées afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux, ainsi que de l'évolution des risques de sécurité de l'information afférents.
k) **Responsabilité et imputabilité :** L'efficacité des mesures de sécurité de l'information exige l'attribution claire des responsabilités à tous les niveaux de l'organisation et la mise en place de processus de gestion de la sécurité de l'information permettant une reddition de comptes adéquate.
l) **Transparence :** L'information concernant les événements de sécurité, les pratiques et les solutions de sécurité de l'information afférentes doit être communiquée avec fluidité au sein de l'Administration publique, sous réserve du droit applicable.
m) **Universalité :** Les pratiques et les solutions retenues en matière de sécurité de l'information doivent correspondre, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale.

4. ORGANISATION DE LA SÉCURITÉ DE L'INFORMATION

La gestion de la sécurité de l'information repose sur une compréhension commune et sur une approche globale qui prend en compte les dimensions humaines, organisationnelles, financières, juridiques et technologiques.

Cette gestion nécessite la mise en place de mesures adaptées à la réalité et aux activités du Musée, encadrées par des exigences de sécurité et des pratiques reconnues, tout en laissant au Musée la latitude quant au choix des moyens pour leur mise en œuvre.

5. GESTION INTÉGRÉE DES RISQUES DE SÉCURITÉ DE L'INFORMATION

La gestion intégrée des risques liés à la sécurité de l'information est une responsabilité organisationnelle qui repose sur un principe d'amélioration continue et qui vise l'identification, l'analyse et le traitement des risques à tous les niveaux hiérarchiques.

Dans le cadre de sa gestion intégrée des risques et à l'aide de divers outils de gestion, le Musée identifie et évalue régulièrement les risques pouvant compromettre la disponibilité, l'intégrité et la confidentialité de l'information et met en place des mesures pour réduire ces menaces. Il met en œuvre des processus de gestion qui assurent le respect des exigences en matière de sécurité de l'information ainsi que l'adoption des pratiques reconnues. Ceux-ci comprennent aussi la conduite d'Évaluations des facteurs à la vie privée conformément à sa *Politique d'accès à l'information et de protection des renseignements personnels*, pour évaluer les risques en lien avec la sécurité des renseignements personnels dans le cadre de la mise en place de système ou du développement de projets les concernant.

6. GESTION DES ACTIFS

Le niveau de protection et les moyens mis en œuvre par le MAC afin d'assurer la protection de ses actifs informationnels doivent être proportionnels à leur valeur pour l'organisation et à leur classification de sécurité. Cette protection doit être assurée tout le long de leur cycle de vie.

L'ensemble des actifs informationnels du MAC doit être identifié et classifié conformément au *modèle de classification de sécurité des données numériques gouvernementales* (arrêté numéro 2024-05). Le MAC doit mettre en place les outils, directives, procédures, moyens technologiques nécessaires à son application, ainsi qu'assurer la tenue d'un registre consignant les informations sur la classification de sécurité des données. Les responsabilités liées à l'application de la classification sont partagées comme suit :

- Le sous-comité de classification de sécurité effectue l'analyse des préjudices et l'attribution du profil de mesures de sécurité aux données structurées
- La personne détentrice responsable de l'actif, appuyée par la responsable de la gestion documentaires, effectue l'analyse des préjudices et applique le marquage correspondant aux données non structurées,

Le cycle de vie des actifs informationnels du Musée est encadré par sa Politique de gestion de l'information, ainsi que la Politique d'accès aux documents et de protection des renseignements personnels.

7. ENGAGEMENT DES PERSONNES UTILISATRICES

L'atteinte d'un niveau de sécurité acceptable pour le Musée repose sur une vision commune et sur l'engagement continu de toutes les personnes utilisatrices ayant accès aux actifs informationnels du Musée.

À cet effet, toute personne nouvellement employée par le Musée, prestataire de services ou autre tierce partie doit :

- Lire et s'engager formellement à respecter les principes directeurs de la Politique (voir Annexe 1) ;
- Prendre connaissance et signer l'entente de sécurité et de confidentialité pour l'accès aux actifs informationnels du Musée.

8. CONTRÔLE DES ACCÈS

Le contrôle des accès vise à sécuriser les actifs informationnels lors de leur utilisation. À cet effet, le MAC :

- S'assure que les personnes utilisatrices disposent uniquement des accès autorisés nécessaires à l'exercice de leurs fonctions ;
- Rend chaque détentrice ou détenteur ou propriétaire d'actif informationnel responsable d'autoriser les accès à cet actif ;
- Déploie, par l'entremise du service des technologies de l'information, les mécanismes techniques nécessaires (identification, authentification, traçabilité), applique les accès approuvés par les propriétaires d'actifs et met en œuvre les mesures de sécurité correspondant au marquage ou au profil de mesures de sécurité attribué à l'actif.
- Rend chaque personne utilisatrice responsable de la protection de ses informations d'authentification ;
- Veille à ce que les droits d'accès soient retirés à la fin de la relation contractuelle ou ajustés en cas de changement de rôle ;
- Restreint l'accès à la gestion du code source des programmes.

9. RELATION AVEC LES TIERCES PARTIES

Le Musée doit garantir la protection des actifs informationnels accessibles aux tierces parties.
À cet effet, il :

- Définit avec les tierces parties les exigences de sécurité de l'information afin de limiter les risques liés à leurs accès et s'assure que ces exigences sont documentées ;
- Intègre dans les contrats et ententes des clauses précises concernant la sécurité de l'information et la gestion des risques associés à la chaîne d'approvisionnement des produits et services, quel que soit le support (numérique, papier ou tout autre format) ;
- Formalise les accords conclus avec les tierces parties en incluant des dispositions visant la protection des actifs informationnels ;
- Surveille et révise régulièrement la prestation des services assurés par les tierces parties ;
- Gère les changements apportés aux prestations de service afin de maintenir la conformité aux exigences de sécurité.

10. SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

Le Musée doit s'assurer de protéger ses actifs informationnels contre les risques physiques. À cet effet, il :

- Empêche tout accès physique non autorisé ainsi que toute intrusion ou dommage pouvant compromettre l'information ou les moyens de traitement ;
- Protège les actifs contre la perte, l'endommagement, le vol ou la compromission, ainsi que contre toute interruption des activités ;
- Configure de manière sécuritaire les équipements ou postes de travail situés dans des zones ouvertes afin de réduire les risques qu'ils peuvent représenter pour l'organisation.

11. SÉCURITÉ LIÉE À L'EXPLOITATION

Le Musée :

- S'assure de l'exploitation adéquate et sécurisée de ses actifs informationnels afin de limiter les risques liés aux pannes des systèmes ;

- Garantit la protection des informations et des moyens de traitement contre les cyberattaques, la perte de données et toute exploitation des vulnérabilités techniques, y compris celles pouvant toucher les actifs physiques ;
- Met en place des mécanismes permettant l'enregistrement des événements et la génération de preuves, ainsi que la sauvegarde régulière des données et la surveillance continue des actifs informationnels.

12. SÉCURITÉ DES COMMUNICATIONS

Le Musée garantit la protection de l'information circulant sur ses réseaux internes et veille au maintien de la sécurité des données transférées à l'intérieur de l'organisation ainsi qu'avec toute entité externe.

13. ACQUISITION, DÉVELOPPEMENT ET MAINTENANCE

Pour limiter les risques opérationnels liés à la sécurité de l'information, tout actif doit respecter le principe de sécurité par défaut et demeurer sécurisé grâce aux efforts de maintenance. Le Musée :

- Veille à ce que la sécurité de l'information soit intégrée aux systèmes tout au long de leur cycle de vie, incluant des exigences spécifiques pour les systèmes offrant des services sur des réseaux publics ;
- S'assure que les enjeux de sécurité sont pris en compte et traités dans le cadre du cycle de développement des systèmes d'information ;
- Établit des règles visant à garantir la disponibilité, l'intégrité et la confidentialité des systèmes et des données.

14. GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

Le Musée garantit une méthode cohérente et efficace de gestion des incidents, incluant la communication des événements et des failles liés à la sécurité de l'information. À cet effet, il se dote d'une directive en matière de gestion des incidents de sécurité de l'information qui :

- Établit des responsabilités et des procédures permettant une réponse rapide, efficace et appropriée en cas d'incident ;
- Guide le signalement, dans les meilleurs délais, des événements liés à la sécurité de l'information par les voies appropriées ;
- Dirige tout membre du personnel, tierce partie ou autre personne utilisatrice des systèmes et services du Musée à signaler toute faille de sécurité observée ou soupçonnée ;
- Propose un cadre pour évaluer les événements liés à la sécurité de l'information afin de déterminer s'ils doivent être classés comme incidents ;
- Prescrit la mise en œuvre de mesures correctives pour prévenir la récurrence et garantir le retour à un niveau de sécurité acceptable ;
- Encadre la collecte sécuritaire des preuves nécessaires à l'analyse et au traitement des incidents.

Le Musée s'est également doté d'une procédure et d'un registre pour encadrer le traitement des incidents de confidentialité en matière de renseignements personnels.

15. GESTION DE LA CONTINUITÉ

Le Musée s'assure du maintien de ses services par la mise en place d'un processus de prévention des menaces et de continuité des activités. À cet effet, il :

- Détermine ses exigences en matière de sécurité de l'information et de continuité dans des situations défavorables, telles qu'une crise ou un sinistre ;
- Veille à ce que l'ensemble des processus, procédures et mesures de continuité soient régulièrement révisé afin d'assurer le niveau requis de sécurité de l'information en situation défavorable.
- Vérifie régulièrement l'efficacité des mesures de continuité mises en place afin de s'assurer qu'elles demeurent valides et adaptées.

Pour chacun des systèmes critiques du Musée, le détenteur ou propriétaire de l'actif concerné doit élaborer un Plan de continuité des affaires (PCA), en assurer la mise à jour régulière et veiller à ce qu'il soit périodiquement testé par les utilisateurs afin d'en confirmer la pertinence et l'efficacité.

16. CONFORMITÉ

Le Musée doit veiller à éviter toute violation des obligations légales, réglementaires ou contractuelles relatives à la sécurité de l'information. À cet effet, il :

- Identifie la législation et les exigences contractuelles applicables ;
- Assure la protection de la propriété intellectuelle, des enregistrements, de la vie privée et des données à caractère personnel ;
- Procède à des revues indépendantes et périodiques de la sécurité de l'information ;
- Participe aux activités de conformité internes et externes avec les politiques et normes de sécurité ;
- Vérifie régulièrement la conformité technique des systèmes.

17. SANCTIONS

- Lorsqu'une personne utilisatrice contrevient à la Politique ou aux directives qui en découlent, elle s'expose, selon la gravité du manquement, à des mesures disciplinaires, administratives ou légales.
- Les tierces parties peuvent être soumises à des mesures administratives, telles que la résiliation du contrat ou la suspension de son mandat auprès du Musée.
- Tout manquement à la sécurité de l'information est porté à l'attention du Support informatique du Musée pour vérification. Le Support informatique s'assure d'acheminer le signalement d'un manquement à la direction ou à toute autre personne désignée par le Musée qui est responsable d'assurer la mise en place de mesures correctives appropriées (voir la section 19).

18. DROIT DE REGARD

Le Musée, en conformité avec la législation et la réglementation en vigueur, exerce un droit de regard sur tout usage de ses actifs informationnels. Il peut mettre en place des mécanismes, tels que des outils technologiques, des vérifications ou des audits, afin de s'assurer de l'application appropriée de la Politique et des directives ou autres documents normatifs qui en découlent.

19. RÔLES ET RESPONSABILITÉS

La sécurité de l'information repose sur une structure de gouvernance claire et une répartition explicite des responsabilités au sein du Musée. Les rôles décrits ci-dessous définissent les responsabilités générales en matière de sécurité de l'information, sans préjudice des directives et procédures opérationnelles adoptées par le Musée.

Le Musée demeure responsable de la sécurité de l'information dans toute forme d'impartition. Il doit, à ce titre, préciser ses exigences en matière de sécurité de l'information dans toute entente ou tout contrat conclu avec un partenaire interne ou externe.

Conseil d'administration	• Adopter la Politique; • S'assurer de l'existence d'un cadre de gouvernance adéquat en sécurité de l'information ; • Recevoir l'information pertinente concernant les risques informationnels majeurs et les incidents significatifs.
Comité d'audit du CA	• Exercer un rôle de surveillance en matière de sécurité de l'information ; • Prendre connaissance des risques informationnels prioritaires et les incidents significatifs ; • Effectuer, au besoin, des redditions au CA en ces matières.
Direction générale	• Assumer la responsabilité ultime de la sécurité de l'information relevant de son autorité ; • Veiller à la mise en place et au maintien d'un cadre de gouvernance en cette matière, conforme aux lois et orientations gouvernementales applicables ; • Désigner les responsables requis en matière de sécurité de l'information et de protection des renseignements personnels, ainsi que les membres des instances internes de gouvernance en ces matières ; • S'assurer de la disponibilité des ressources nécessaires à l'application de la Politique.
Comité de direction	• Assurer la coordination organisationnelle en matière de sécurité de l'information ; • Contribuer au suivi des enjeux et des risques informationnels ayant un impact sur le Musée, conformément aux orientations approuvées.
Direction des technologies	• Développer, actualiser et soutenir l'application de la Politique et des directives en découlant; • Mettre en œuvre, dans son champ de responsabilités, les mesures de sécurité approuvées par le Musée, conformément aux directives en vigueur et aux exigences gouvernementales applicables.
Direction des ressources humaines	• Contribuer à l'application de la Politique en intégrant les exigences de sécurité aux processus de gestion du personnel ; • Collaborer dans la mise en œuvre de programmes de sensibilisation et de la formation du personnel ; • Soutenir la mise en œuvre des mesures administratives prévues en cas de non-respect, conformément aux directives en vigueur.
Secrétariat général	• Appuyer le développement et l'actualisation de la Politique en veillant au respect des obligations légales liées à l'information et à la protection des renseignements personnels.

Direction des collections et des ressources documentaires	• Contribuer aux mécanismes de gouvernance documentaire et de protection des renseignements personnels, conformément aux directives en vigueur.
Personnes utilisatrices (employées et employés du Musée et tierces parties)	• Appliquer la Politique dans leurs activités. • Protéger l'information conformément à son niveau de sensibilité. • Autoriser et utiliser les accès selon le principe du besoin de connaître. • Signaler sans délai tout incident ou situation à risque.
Cheffe ou chef de la sécurité de l'information organisationnelle (CSIO)	• Coordonner la mise en œuvre des orientations stratégiques en matière de sécurité de l'information ; • Veiller au respect de la Politique, des directives en découlant et des autres documents d'encadrement applicables ; • Superviser l'élaboration et la mise en œuvre des mesures de protection des actifs informationnels ; • Intégrer la sécurité de l'information dans les projets; • Collaborer avec la personne responsable de la gestion contractuelle pour s'assurer que les contrats formels et les documents guidant les acquisitions de biens et des services incluent des clauses et considérations garantissant la sécurité des actifs informationnels ; • Mettre en place un processus de gestion des risques liés à la sécurité de l'information ; • Assurer la sensibilisation et la formation du personnel ; • Collaborer avec les instances de gouvernance et les parties prenantes pour renforcer la sécurité, réduire les risques et promouvoir la conformité ; • Communiquer toute situation à risque ou tout incident majeur aux autorités compétentes et veiller à la mise en œuvre des mesures correctives.
Coordinateur organisationnel des mesures de sécurité de l'information (COMSI)	• Soutenir la personne nommée CSIO en lui fournissant l'expertise technique nécessaire ; • Collaborer à la mise en œuvre des processus de gestion des menaces, vulnérabilités et incidents ; • Informer rapidement la ou le CSIO et les instances compétentes de tout évènement présentant un risque ; • Participer à l'élaboration de programmes de sensibilisation et de formations du personnel ; • Assurer une collaboration continue afin de renforcer la posture de sécurité et de garantir la conformité.
Le centre opérationnel de sécurité de l'information (COSI)	• Surveiller et analyser les alertes de sécurité ; • Prioriser les incidents pour réduire les impacts sur le Musée ; • Coordonner la réponse aux incidents ; • Vérifier la correction des failles ; • Maintenir une veille active sur les menaces et vulnérabilités.

Comité de sécurité de l'information (CSI)	• Agir comme instance de concertation en matière de sécurité de l'information ; • Examiner et formuler des recommandations concernant les orientations, politiques et plans d'action ; • Veiller à la prise en charge des risques, des vulnérabilités et des incidents identifiés ; • Encadre la mise en œuvre de la classification de sécurité des données ; • Analyser les évènements ayant compromis ou pouvant compromettre la sécurité de l'information et proposer des actions correctives.
Responsable de l'accès aux documents et de la protection des renseignements personnels	• Assurer la conformité du Musée à ses obligations en matière de protection des renseignements personnels ; • Recevoir et traiter les signalements d'incidents de confidentialité en lien avec les renseignements personnels et proposer des actions correctives.
Chef de la gestion d'immeuble et de la sécurité	Assurer la sécurité physique de l'information, soit : • Mettre en place les mesures de protection physiques des locaux et de sécurisation de leurs accès, notamment lorsqu'ils abritent des systèmes et des installations technologiques stratégiques ou essentiels ou des supports d'information confidentielle; • Concevoir et mettre en œuvre les mesures de protection physique des biens contre les sinistres, les pertes, les dommages, le vol ainsi que l'interruption des activités du MAC; • S'assurer de la mise au rebut sécuritaire des supports de l'information; • S'assurer que les salles des serveurs, salles de télécommunication, salles des archives de la collection et salles des archives institutionnelles sont uniquement accessibles aux utilisateurs autorisés; • Élaborer et mettre en œuvre des directives, des guides et des procédures propres à son domaine d'intervention et nécessaires afin d'assurer la sécurité de l'information.

20. DÉFINITIONS

Aux fins de la Politique, il est entendu par :

a) **Musée ou MAC** : Le Musée d'art contemporain de Montréal, société d'État responsable de la gestion des actifs informationnels visés par la Politique.
b) **Actifs informationnels**: Ensemble des informations ayant une valeur pour l'organisation qui en est détentrice et dont la gestion doit être assurée de manière stratégique, notamment par la mise en place d'un système de classement, de mesures de sécurité particulières et d'un cycle de vie préétabli.
c) **Données non structurées** : Donnée stockée sans être organisée de manière prédéfinie, ce qui rend son utilisation plus difficile pour un système d'information. Les fichiers de type PDF, Word, Excel, PowerPoint, les fichiers audio, vidéo ou image, ainsi que les courriels sont des exemples de données non structurées.

d) **Données structurées** : Donnée stockée selon un format prédéfini de façon à permettre son interprétation par un logiciel. Les données semi-structurées dans un format préétabli, afin de permettre leur utilisation par un système d'information (json, xml, csv, etc.), ainsi que les DMU, sont considérées comme des données structurées en vertu du modèle de classification.
e) **Besoin de connaître** : Accès aux actifs informationnels accordé uniquement lorsque requis pour l'exercice des fonctions d'un mandat.
f) **Moindre privilège** : Accès donné à une personne utilisatrice, un processus ou un système, uniquement selon un niveau minimal d'accès nécessaire pour accomplir des tâches ou des responsabilités précises.
g) **Information sensible** : Information dont la divulgation, la perte ou l'altération non autorisée pourrait causer un préjudice au Musée, à ses partenaires ou à des personnes, incluant les renseignements personnels. Dans la Politique, elle correspond principalement aux informations qualifiées « hautement confidentielles » et « confidentielles ».
h) **Renseignement personnel** : Information concernant une personne physique permettant de l'identifier, directement ou indirectement, au sens des lois applicables.
i) **Personnes utilisatrices** : L'ensemble des personnes accédant aux systèmes, aux réseaux ou aux actifs informationnels du Musée incluant les employées, employés et les tierces parties.
j) **Propriétaire de l'information** : Direction ou unité administrative responsable d'un ensemble d'informations qui en détermine la sensibilité, les règles d'accès et les usages autorisés.
k) **Incident de sécurité de l'information** : Événement réel ou suspecté compromettant ou susceptible de compromettre la confidentialité, l'intégrité ou la disponibilité d'un actif informationnel (ex. : accès non autorisé, logiciel malveillant, perte de données).
l) **Incident de confidentialité** : Situation où des renseignements personnels sont consultés, utilisés, diffusés, perdus ou détruits de manière non autorisée, au sens du *Règlement sur les incidents de confidentialité* et de la Loi.
m) **Tierce partie** : Toute personne ou organisation externe au Musée (partenaire, artiste, consultante ou consultant, prestataire, bénévole, stagiaire, membre du CA et de ses comités, etc.) autorisée à accéder à des actifs informationnels ou à des systèmes, dans le cadre d'un mandat ou d'une collaboration.

21. ENTRÉE EN VIGUEUR ET RÉVISION

La Politique est entrée en vigueur à la date de son adoption par le CA du Musée, le 19 mars 2026, résolution 1605.

Elle est révisée périodiquement ou lors de tout changement législatif, organisationnel ou technologique majeur.

ANNEXE 1 : ACCUSÉ DE RÉCEPTION DE LA POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Je, _____, employée ou employé, stagiaire, bénévole, cadre ou membre du conseil d'administration du Musée d'art contemporain de Montréal, reconnais avoir reçu un exemplaire de la *Politique de sécurité de l'information* de l'organisation.

Je déclare, par la présente, avoir lu cette Politique et avoir bien compris son contenu.

Je comprends que toute violation de cette Politique peut entraîner des mesures administratives ou disciplinaires.

Signature : _____

Date : _____

Les renseignements personnels collectés par le MAC dans ce formulaire seront utilisés aux fins suivantes : confirmer votre adhésion à la présente politique et aux fins d'archivage. La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels vous permet de demander accès à vos renseignements personnels ou, dans certains cas, de demander leur rectification. Pour exercer ces droits, contactez la responsable de l'accès aux documents et de la protection des renseignements personnels du MAC à jennifer.dorner@macm.org.
Pour d'avantage information sur les procédures en place en lien avec les renseignements personnels, visitez : https://macm.org/conditions-utilisation/