mpac Société d'évaluation foncière des municipalités[MC]

Politique de sécurité de l'information

mpac

Information Security Policy

1. But et objectifs

La présente politique établit les exigences visant à protéger les informations, les systèmes et les actifs de l'organisation. Elle garantit la confidentialité, l'intégrité et la disponibilité des données, tout en soutenant le respect des obligations légales, réglementaires et contractuelles.

2. Portée et application

2.1 Définition de la sécurité de l'information

La sécurité de l'information protège les informations et les systèmes contre tout accès, utilisation, divulgation, modification et interruption non autorisés, garantissant ainsi la confidentialité, l'intégrité et la disponibilité des données.

2.2 Approche en matière de sécurité de l'information

La sécurité est la responsabilité de tous. L'organisation adopte les pratiques de la norme ISO 27001 pour guider la mise en œuvre et l'amélioration continue.

2.3 Structure du présent document

Les mesures de contrôle sont regroupées selon quatre catégories, soit les aspects :

- organisationnels;
- humains;
- physiques;
- technologiques.

3. Responsabilités

3.1 Employés

Les employés sont tenus de respecter toutes les politiques pertinentes, de suivre la formation en sécurité de l'information et de signaler sans délai toute violation de politique à leur gestionnaire.

3.2 Gestionnaire

Les employés et les gestionnaires sont tenus de respecter l'ensemble des exigences de la politique, de suivre la formation en matière de sécurité requise, d'assurer la responsabilisation et la compétence du personnel, de veiller au respect de la politique et de traiter toute violation relevant de leur champ de responsabilité.

3.3 Chef de service
Il tient le personnel responsable de ses obligations en vertu de la politique, veille à la conformité des employés sous sa responsabilité directe, contribue aux mises à jour de la politique et traite toute situation de non-conformité dans son secteur.

3.4 Directeur de la cybersécurité
Le directeur de la cybersécurité est responsable d'enquêter sur les cas de non-conformité en collaboration avec les services concernés, de surveiller et d'évaluer l'efficacité de la politique, de recommander des mises à jour, de fournir des orientations quant à l'interprétation et à l'application de la politique, et d'appuyer les initiatives de formation afin d'assurer sa mise en œuvre et son respect.

3.5 Vice-président et directeur des technologies de l'information
Il supervise les rapports de conformité à la politique destinés à la haute direction et veille à ce que tous les employés soient informés de la politique.

3.6 Président et chef de l'administration
Le président et chef de l'administration est responsable de veiller à ce que les employés relevant directement de lui respectent la politique, d'approuver la politique et toute modification qui y est apportée et de traiter les situations de non-conformité conformément à la présente politique et aux autres politiques organisationnelles applicables.

3.7 Fournisseurs et prestataires tiers
Les fournisseurs et les prestataires tiers doivent protéger les données organisationnelles, appliquer les mesures de sécurité définies par la politique et les contrats, signaler sans délai tout incident impliquant des données de la SEFM et veiller à ce que leurs sous-traitants respectent des contrôles de sécurité équivalents ou plus rigoureux.

4. Références
ISO 27001, ISO 27002, cadre de cybersécurité du NIST et directives de la Cloud Security Alliance (CSA).

5. Mesures de contrôle organisationnelles
5.1 Politiques en matière de sécurité de l'information

5.1.1 L'organisation élabore, diffuse et communique ses politiques et normes de sécurité de l'information approuvées aux employés et aux groupes externes concernés. Ces politiques et normes font l'objet d'évaluations régulières afin d'en vérifier la pertinence, l'exhaustivité,

les possibilités d'amélioration et l'efficacité, notamment à des moments prévus ou à la suite de changements majeurs. Des contrôles de sécurité de l'information sont mis en place à l'échelle de l'organisation afin d'assurer le respect de ces politiques.

5.2 Rôles et responsabilités en matière de sécurité de l'information

5.2.1 L'organisation désigne les rôles et les responsabilités. Elle supervise les principaux processus de sécurité de l'information. Les propriétaires des données fournissent les ressources nécessaires et mettent en place des contrôles de sécurité. Bien que les propriétaires des données puissent déléguer des tâches, ils en restent responsables.

5.3 Séparation des fonctions

5.3.1 La séparation des fonctions a pour objectif de réduire le risque de fraude, d'erreurs et de contournement des contrôles de sécurité. Pour ce faire, il convient de veiller à ce que les fonctions incompatibles soient gérées par différentes personnes, en établissant des processus clairs pour l'octroi et l'élévation des accès, et en séparant les rôles incompatibles dans la mesure du possible.

5.4 Responsabilités de la direction

5.4.1 La direction est chargée de veiller à ce que les employés, les sous-traitants et les consultants comprennent et respectent leurs responsabilités en matière de sécurité de l'information. L'organisation communique clairement ces responsabilités aux nouveaux membres du personnel, offre une formation complète sur les politiques de sécurité de l'information et tient le personnel informé des mises à jour importantes de ces politiques. En outre, des formations de mise à niveau continues sont offertes à l'ensemble du personnel afin de tenir compte des menaces actuelles et de toute modification importante du cadre de sécurité de l'information.

5.5 Autorités externes et groupes d'intérêt spéciaux

5.5.1 L'organisation assure une communication efficace en matière de sécurité de l'information avec les autorités légales, réglementaires et de surveillance en établissant des processus clairs et en maintenant des contacts appropriés.

5.5.2 Elle participe également activement à des groupes d'intérêt spéciaux et à des forums afin de se tenir informée des meilleures pratiques, de recevoir des alertes en temps opportun concernant les menaces et les vulnérabilités, et d'améliorer ses capacités de réponse aux incidents grâce à des canaux de communication établis.

5.6 Renseignements sur les menaces

5.6.1 L'organisation vise à améliorer sa connaissance de son environnement de menaces afin de permettre une atténuation et une prévention efficaces des menaces et d'en réduire les répercussions.

5.7 Sécurité de l'information dans la gestion de projet

5.7.1 La gestion de projet doit prendre en compte les risques liés à la sécurité de l'information tout au long du cycle de vie du projet en évaluant les risques dès le départ, en intégrant les exigences de sécurité dès le début et en cernant rapidement les mesures de contrôle nécessaires.

5.8 Inventaire de l'information et des actifs connexes

5.8.1 L'organisation tient à jour un inventaire de l'information et des actifs connexes, attribue la responsabilité de leur sécurité et consigne les renseignements relatifs aux actifs afin d'en assurer la protection et la responsabilisation.

5.9 Utilisation acceptable

5.9.1 L'organisation établit des règles et des procédures claires afin d'assurer une utilisation et une manipulation appropriées et sécuritaires de l'information et des actifs technologiques.

5.10 Restitution des actifs

5.10.1 L'organisation doit identifier clairement et documenter l'ensemble de l'information et des autres actifs connexes devant être restitués.

5.11 Classification et étiquetage de l'information

5.11.1 L'information doit être classée et étiquetée afin d'assurer une protection adéquate en fonction de son importance pour l'organisation.

5.11.2 La classification incombe aux propriétaires et tient compte de la confidentialité, de l'intégrité et de la disponibilité de l'information. Elle est déterminée par les répercussions potentielles d'une compromission.

5.12 Transfert de l'information

5.12.1 Cette section souligne la nécessité d'assurer le transfert sécurisé de l'information, tant à l'intérieur de l'organisation qu'avec les parties externes, en mettant l'accent sur la conclusion d'ententes formelles, la protection des communications électroniques et le maintien de l'information au Canada.

5.13 Gestion des accès et des identités

5.13.1 Les informations d'authentification doivent être attribuées formellement, et il incombe aux utilisateurs de les protéger et d'utiliser des mots de passe robustes.

5.13.2 Les droits d'accès doivent être gérés au moyen de processus formels, faire l'objet de révisions régulières et être révoqués ou ajustés à la suite de changements liés à l'emploi.

5.13.3 Pour les fournisseurs, les exigences en matière de sécurité doivent être documentées et des processus doivent être mis en place afin de traiter les risques liés à l'accès des fournisseurs et à leurs produits.

5.14 Sécurité des fournisseurs, du nuage et de la chaîne d'approvisionnement des TIC

5.14.1 L'organisation doit établir et documenter des exigences claires en matière de sécurité de l'information dans l'ensemble de ses relations avec les fournisseurs, y compris dans les ententes et les dispositifs relatifs à la chaîne d'approvisionnement des technologies de l'information et des communications (TIC).

5.14.2 Ce processus implique de cerner et d'atténuer les risques, de définir et de surveiller les niveaux de service, et de s'assurer que les deux parties comprennent leurs obligations en matière de sécurité.

5.14.3 En ce qui concerne les services infonuagiques, l'organisation doit mettre en œuvre des politiques de sécurité pertinentes et les communiquer aux intervenants.

5.15 Gestion des incidents

5.15.1 L'organisation doit établir des procédures claires pour la gestion des incidents de sécurité, notamment la définition des rôles et des processus de signalement. Les incidents doivent être classés par catégorie et hiérarchisés, et des plans d'intervention efficaces doivent être communiqués à tous les intervenants. Les leçons tirées des incidents doivent servir à orienter les améliorations futures. Des procédures adéquates de collecte des preuves sont essentielles aux fins d'actions juridiques et disciplinaires.

5.16 Continuité des activités et état de préparation aux TIC

5.16.1 La sécurité de l'information et l'état de préparation aux TIC en cas de perturbation visent à protéger les actifs de l'organisation et à garantir leur disponibilité. Les contrôles de sécurité doivent être adaptés et intégrés aux plans de continuité des activités, l'état de préparation aux TIC assurant la continuité des activités même en cas de perturbation.

5.17 Conformité, propriété intellectuelle, gestion des documents et protection de la vie privée

5.17.1 L'organisation doit se conformer aux obligations légales, réglementaires et contractuelles en matière de sécurité de l'information, de propriété intellectuelle et de gestion des documents.

5.17.2 Elle protège les documents et les renseignements personnels identifiables contre l'accès non autorisé, la perte et l'utilisation abusive et met en œuvre les contrôles et mesures nécessaires afin de protéger la vie privée et les produits exclusifs.

5.18 Examen indépendant et procédures opérationnelles

5.18.1 L'organisation assure la sécurité de l'information au moyen d'examens indépendants réguliers, du respect des politiques et des normes établies et de la consignation de procédures opérationnelles accessibles pour le traitement de l'information.

6. Mesures de contrôle liées aux personnes

6.1 Présélection

6.1.1 La présélection vise à s'assurer que l'ensemble du personnel est apte à exercer ses fonctions et conscient de ses responsabilités. L'organisation procède à des vérifications d'intégrité et d'éthique et recueille les renseignements relatifs aux candidats conformément aux lois en vigueur.

6.2 Conditions d'emploi

6.2.1 L'ensemble du personnel doit être informé de ses responsabilités en matière de sécurité de l'information, tant avant l'entrée en fonction qu'au moment de l'embauche.

6.3 Sensibilisation, formation et perfectionnement en matière de sécurité

6.3.1 L'ensemble du personnel et des parties concernées doit recevoir régulièrement de la formation et des mises à jour sur leurs responsabilités en matière de sécurité de l'information, les menaces actuelles, les modifications aux politiques et, pour les équipes techniques, un perfectionnement des compétences adapté à leurs fonctions.

La formation est offerte périodiquement et actualisée au besoin.

6.4 Processus disciplinaire

6.4.1 Le processus disciplinaire vise à s'assurer que toutes les personnes comprennent les conséquences d'une violation des politiques de sécurité de l'information. Les mesures disciplinaires ne sont prises qu'après la confirmation d'une violation et tiennent compte des exigences légales et opérationnelles. Ce processus sert à la fois de mesure dissuasive et de mécanisme de traitement des violations et permet une intervention immédiate en cas de manquement délibéré.

6.5 Responsabilités après la cessation d'emploi

6.5.1 Le processus de gestion de la cessation d'emploi ou du changement d'affectation doit préciser quelles responsabilités et obligations en matière de sécurité de l'information demeurent applicables après la cessation ou le changement.

6.6 Accords de confidentialité ou de non-divulgation

6.6.1 Les accords doivent garantir la protection des renseignements confidentiels tant pour le personnel que pour les parties externes. Ces accords doivent faire l'objet de révisions périodiques et être mis à jour au besoin.

6.7 Télétravail

6.7.1 Le travail à distance désigne l'accès, par le personnel, aux informations de l'organisation à partir de lieux situés à l'extérieur des locaux officiels, notamment le « télétravail », le « travail à distance », le « lieu de travail flexible », les « environnements virtuels » et la « maintenance à distance ». L'objectif est d'assurer le maintien de la sécurité de l'information dans le cadre de ces modalités de travail.

6.8 Signalement des événements de sécurité de l'information

6.8.1 Il convient d'assurer un signalement rapide et efficace des événements de sécurité de l'information par l'ensemble du personnel afin de prévenir les incidents ou d'en réduire les répercussions.

7. Mesures de contrôle physiques

7.1 Sécurité physique et surveillance

7.1.1 Périmètres de sécurité physique : définir et tester régulièrement les limites de sécurité afin d'empêcher tout accès non autorisé, tout dommage ou toute interférence.

7.1.2 Entrée physique : contrôler tous les points d'accès, en particulier les zones de livraison et de chargement afin de restreindre l'entrée aux personnes autorisées uniquement.

7.1.3 Sécurisation des bureaux, des locaux et des installations : mettre en place des mesures de contrôle physique pour protéger les actifs de l'organisation contre tout accès non autorisé ou tout dommage.

7.1.4 Surveillance de la sécurité physique : utiliser des systèmes de surveillance tels que des agents de sécurité, des alarmes, des systèmes de vidéosurveillance ou des logiciels de gestion de la sécurité afin de surveiller et de dissuader tout accès non autorisé.

7.2 Protection contre les menaces physiques et environnementales

7.2.1 L'organisation doit recenser et gérer les risques liés aux menaces physiques et environnementales comme les incendies, les inondations, les tremblements de terre, les troubles civils ou les déchets toxiques, mettre en place des mesures de protection, surveiller l'évolution de ces risques et faire appel à des spécialistes au besoin.

7.3 Zones sécurisées

7.3.1 Les mesures de sécurité applicables au travail dans les zones sécurisées doivent s'appliquer à l'ensemble du personnel et couvrir toutes les activités qui s'y déroulent.

7.4 Bureau et écran dégagés

7.4.1 L'organisation doit établir et communiquer une norme relative aux bureaux et écrans dégagés à l'ensemble des parties intéressées concernées.

7.5 Protection des équipements et des supports

7.5.1 Ces sections soulignent la nécessité de disposer de directives visant à protéger les équipements contre les menaces physiques et environnementales, à sécuriser les actifs de l'organisation utilisés hors site avec l'autorisation de la direction, et à gérer et éliminer de manière sécurisée les supports de stockage afin d'empêcher tout accès non autorisé ou toute perte d'information.

7.6 Services publics, câblage, maintenance et élimination

7.6.1 Cette section décrit les directives officielles visant à protéger les actifs et l'information de l'organisation contre les risques liés aux défaillances des services publics, aux problèmes de câblage, aux lacunes dans la maintenance des équipements, ainsi qu'à l'élimination ou à la réutilisation inadéquates des équipements.

7.6.2 Elle met l'accent sur la protection des services publics (électricité, télécommunications, etc.), la sécurisation des câblages d'alimentation et de communication, la maintenance des équipements au moyen de contrôles appropriés et l'élimination ou la réutilisation sécurisée des dispositifs afin de prévenir toute fuite d'information.

8. Mesures de contrôle technologiques

8.1 Dispositifs utilisateurs

8.1.1 Dispositifs utilisateurs : établir et communiquer des normes de configuration sécurisées pour les dispositifs des utilisateurs, en veillant à ce que tous les utilisateurs comprennent et respectent les procédures de sécurité.

8.2 Contrôle des accès privilégiés et du code source

8.2.1 L'organisation doit contrôler de façon stricte les droits d'accès privilégié et l'accès à l'information afin de garantir que seuls les utilisateurs, composants et services autorisés disposent des autorisations nécessaires.

8.2.2 L'organisation doit mettre en place des normes relatives au contrôle des accès et à l'accès à l'information afin d'empêcher toute utilisation non autorisée des actifs.

8.2.3 De plus, elle doit restreindre étroitement l'accès au code source et aux outils de développement connexes afin d'assurer la confidentialité et de prévenir toute modification non autorisée.

8.3 Authentification sécurisée

8.3.1 S'assurer que les utilisateurs et les entités sont correctement authentifiés lorsqu'ils accèdent aux systèmes. Utiliser des méthodes d'authentification adaptées à la sensibilité des informations, en privilégiant des techniques plus robustes (p. ex. la biométrie, les jetons) pour les accès à haut risque.

8.4 Gestion des capacités

8.4.1 S'assurer que toutes les installations de traitement de l'information, les ressources humaines et les bureaux disposent d'une capacité suffisante pour répondre aux besoins opérationnels. Déterminer les exigences en fonction du caractère critique des systèmes et des processus.

8.5 Protection contre les logiciels malveillants

8.5.1 La protection contre les logiciels malveillants vise à garantir que l'organisation met en place des contrôles et des activités de sensibilisation des utilisateurs afin de détecter, prévenir et gérer les menaces liées aux logiciels malveillants, et de réduire au minimum le risque que des logiciels malveillants compromettent les actifs informationnels.

8.6 Vulnérabilités techniques

8.6.1 L'organisation vise à prévenir l'exploitation des vulnérabilités techniques en appliquant les correctifs nécessaires, en évitant l'utilisation des mots de passe par défaut des fournisseurs, en effectuant des analyses internes régulières des vulnérabilités sur les systèmes traitant des données confidentielles et en faisant appel à des tiers de confiance pour les analyses externes des systèmes accessibles au public.

8.7 Gestion de la configuration

8.7.1 La gestion de la configuration vise à garantir que l'ensemble du matériel, des logiciels, des services et des réseaux fonctionnent de manière sécurisée et conforme à leur objectif, en imposant des configurations approuvées et en contrôlant toute modification au moyen de rôles et de procédures définis.

8.8 Suppression, masquage et prévention des fuites de données

8.8.1 L'organisation veille à ce que les renseignements sensibles soient supprimés lorsqu'ils ne sont plus nécessaires, limite l'exposition des données personnelles au moyen du masquage ou de l'anonymisation et assure une surveillance des fuites de données afin de prévenir toute divulgation non autorisée.

8.9 Sauvegarde de l'information

8.9.1 L'organisation met en place et teste des stratégies de sauvegarde et de restauration afin de garantir la récupération des données et des systèmes en cas de perte.

8.10 Redondance

8.10.1 L'organisation évalue la nécessité d'une infrastructure de traitement de l'information redondante et, le cas échéant, la maintient afin de répondre à ses exigences de disponibilité.

8.11 Journalisation et surveillance

8.11.1 L'organisation enregistre et protège les données de journalisation, surveille les systèmes afin de détecter les événements de sécurité, se conforme aux exigences légales applicables et conserve les journaux conformément aux obligations en vigueur.

8.11.2 L'organisation surveille régulièrement les systèmes d'information afin de détecter les incidents de sécurité et d'évaluer l'efficacité des mesures de contrôle.

8.12 Synchronisation des horloges

8.12.1 L'organisation doit synchroniser toutes les horloges des systèmes clés à une source de temps unique.

8.13 Programmes utilitaires et installation de logiciels

8.13.1 Seul le personnel autorisé peut utiliser les programmes utilitaires privilégiés, lesquels doivent être clairement identifiés et ne doivent en aucun cas contourner les mesures de sécurité.

8.13.2 Les modifications et installations de logiciels doivent respecter les consignes de sécurité; seules les applications approuvées sont autorisées et les dépendances doivent être maintenues à jour.

8.14 Sécurité réseau, services, segmentation et filtrage Web

8.14.1 Les organisations doivent mettre en œuvre des contrôles stricts afin de protéger l'information et l'infrastructure contre les menaces réseau et les accès non autorisés.

8.14.2 Cela comprend la sécurisation des services réseau, la segmentation des réseaux afin d'établir des périmètres de sécurité et la gestion de l'accès aux sites Web externes dans le but de prévenir les logiciels malveillants et les utilisations non autorisées.

8.15 Utilisation de la cryptographie

8.15.1 La cryptographie est utilisée pour garantir la confidentialité, l'authenticité et l'intégrité des informations. L'organisation évalue les situations où le recours à la cryptographie est

approprié, en limite l'utilisation aux méthodes approuvées et gère les clés cryptographiques de manière sécurisée tout au long de leur cycle de vie.

8.16 Cycle de développement sécurisé

8.16.1 Mettre en œuvre des contrôles de sécurité à toutes les étapes du développement des logiciels et des systèmes, notamment en établissant des règles formelles et des mécanismes de sécurisation appropriés.

8.16.2 Déterminer et traiter les exigences de sécurité lors du développement ou de l'acquisition d'applications.

8.16.3 Appliquer les principes de sécurité aux systèmes.

8.16.4 Appliquer à l'échelle de l'organisation des normes de codage sécurisées pour tous les logiciels nouveaux ou réutilisés. Intégrer des tests de sécurité à chaque phase de développement et vérifier les systèmes avant leur mise en production.

8.16.5 Communiquer clairement les exigences de sécurité aux partenaires de développement externes et en assurer le suivi.

8.16.6 Maintenir une séparation stricte entre les environnements de développement, de test et de production afin de protéger les données de production.

8.16.7 Exiger une approbation formelle et des tests pour toute modification en production afin d'assurer le maintien de la sécurité.

8.16.8 Éviter l'utilisation de données de production réelles à des fins de test. Lorsque cela est inévitable, anonymiser ou modifier les données afin de protéger la vie privée.

8.16.9 Coordonner et contrôler les activités d'audit afin de réduire au minimum les répercussions opérationnelles et de restreindre l'accès aux outils d'audit.

9. Conformité aux politiques

9.1 Exceptions

Exiger une approbation formelle et une acceptation documentée des risques.

9.2 Non-conformité

Peut entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement.

10. Définitions

Information : Connaissance communiquée ou reçue. L'information, sous toutes ses formes (telles que le texte, l'image, la vidéo et la voix), sur tous les supports (tels que le papier, les bandes magnétiques, les disques, les microfilms ou microfiches) et à toutes les

étapes de son cycle de vie (c'est-à-dire créée, saisie, traitée, communiquée, transportée, diffusée, stockée ou éliminée), y compris la description du contenu de l'information, de ses sources, de sa structure et de ses relations, permettant une interprétation correcte de l'information. Les formes et les supports d'information comprennent les technologies actuelles et futures.

Système d'information : Ensemble de personnes, de matériel technologique, de logiciels, de services et de processus automatisés ou non automatisés, organisés afin d'atteindre les objectifs de la SEFM.

SGSI : SGSI signifie Système de gestion de la sécurité de l'information. Il s'agit d'une approche systématique visant à gérer et à protéger les données de la SEFM.

Évaluation des risques : Processus consistant à cerner et à évaluer les risques pertinents pour la SEFM.

Classification des données : Processus de catégorisation des données en fonction de leur niveau de sensibilité et des répercussions pour la SEFM en cas de divulgation, de modification ou de destruction non autorisée.

Vulnérabilité : Faiblesse d'un système informatique pouvant être exploitée par un attaquant.

Incidents de sécurité : Tout incident impliquant la perte, le vol, l'utilisation abusive, l'indisponibilité ou l'accès, l'acquisition, l'utilisation, la divulgation, la modification ou la destruction non autorisés, réels ou présumés, de données de la SEFM, ou toute autre compromission de celles-ci.

Applications métier : Programme informatique conçu pour atteindre les objectifs de la SEFM.

Une application peut être développée à l'interne par la SEFM ou acquise auprès d'un tiers.

Gestion de la continuité des activités : Ensemble des programmes et des activités liés à l'élaboration et au maintien des plans de continuité des activités.