Chambre des notaires

Cadre de sécurité des actifs informationnels

Préparé et sous la responsabilité de la Direction TI
Approuvé le : 8 septembre 2016 par les membres du Conseil d'administration
Par : Sylvie Leclair, directrice générale adjointe – Direction TI

Table des matières

1. Introduction

1.1. Contexte

À titre d'ordre professionnel, la Chambre des notaires du Québec (ci-après, « Chambre des notaires ») a l'obligation d'assurer la protection du public. La sécurité de l'information[1] figure ainsi au cœur des préoccupations de l'organisation[2] et, dans ce contexte, la Chambre des notaires se doit d'élaborer un cadre de sécurité des actifs informationnels[3] et des politiques qui tiennent compte des objectifs de l'organisation et des meilleures pratiques en sécurité de l'information.

Référence: ISO27001:2013(F) 4.1; 4.2, 5.1.

1.2. Objectif

Le présent document constitue le *Cadre de sécurité des actifs informationnels de la Chambre des notaires* (ci-après « cadre de sécurité ») qui établit les pratiques à adopter dans le but de protéger tous les actifs informationnels de l'organisation et de prévenir de potentiels incidents de sécurité[4], incluant la fraude, les fuites d'information, les attaques informatiques, les erreurs accidentelles, les actions délibérées et l'atteinte à la vie privée. De cette manière, la Chambre des notaires protège l'organisation et atténue les risques[5] liés à la confidentialité[6], à l'intégrité[7] et à la disponibilité[8] de l'information[9].

Référence: ISO27001:2013(F) 4.1; 4.2.

1.3. Système de gestion de la sécurité de l'information

Un système de gestion de la sécurité de l'information est une méthode visant à obtenir le niveau de qualité souhaité en assurant la conformité aux exigences telles que définies dans le présent cadre de sécurité. Son application systématise l'établissement de procédures opérationnelles et administratives, leur formalisation et leur communication. Des indicateurs significatifs et une analyse des dysfonctionnements permettent d'apporter des actions préventives et correctives nécessaires en vue de s'inscrire dans une démarche d'amélioration continue.

[1] Voir Annexe 1- Définitions.
[2] *Id*.
[3] *Id*.
[4] *Id*.
[5] *Id.*
[6] *Id*.
[7] *Id*.
[8] *Id*.
[9] *Id*.

1.4. Portée

Le présent cadre de sécurité s'applique à tout actif informationnel détenu par la Chambre des notaires et ses intervenants[10], incluant l'information recueillie dans le cadre d'activités contractuelles, réglementaires et légales.

Aux fins du présent cadre, seront notamment considérés comme intervenants de la Chambre des notaires, son personnel, ses administrateurs, ses sous-traitants, ses fournisseurs, ses partenaires et ses mandataires.

Référence: ISO27001:2013(F) 4.3.

1.5. Engagement du Conseil d'administration

Le présent cadre de sécurité s'inscrit dans un contexte de prévention et de sensibilisation à la sécurité de l'information. Pour ce faire, la collaboration de tous les intervenants est primordiale. Le Comité d'audit et de prospectives financières assure la surveillance de la mise en œuvre du cadre. Le Conseil d'administration s'engage à prendre tous les moyens nécessaires pour soutenir les actions qui doivent être prises dans la mise en œuvre du cadre de sécurité, ainsi que dans la mise en œuvre des politiques et directives afférentes[11].

Référence: ISO27001:2013(F) 5.1.

1.6. Responsable du cadre de sécurité des actifs informationnels

Le présent cadre de sécurité relève du responsable de la sécurité des actifs informationnels. Il doit assurer son maintien, sa révision et sa communication. Le responsable de la sécurité des actifs informationnels est la Directrice générale adjointe des technologies de l'information.

1.7. Surveillance et contrôle des activités

La Chambre des notaires se réserve le droit, sans préavis, de surveiller tout actif informationnel et toute information conservée, traitée et exécutée sur ses systèmes et sur ses appareils mobiles[12].

Si une situation l'exige, la Chambre des notaires assurera un suivi des activités de surveillance, procédera à une investigation sur les irrégularités et en divulguera les résultats aux parties intéressées et concernées.

Référence: ISO27001:2013(F) 5.1.

1.8. Conséquences

Le non-respect du cadre de sécurité peut amener la Chambre des notaires à retirer les droits d'accès à un intervenant ainsi qu'à appliquer des mesures disciplinaires selon les règles

[10] *Id*.
[11] Voir Annexe 2 du présent cadre de sécurité.
[12] Voir Annexe 1 – Définitions.

établies par les ressources humaines, la *Loi sur le notariat*[13] et le *Code des professions*[14]. Tout intervenant qui a connaissance du non-respect ou d'une omission au présent cadre de sécurité doit aviser son gestionnaire ou le responsable de la sécurité des actifs informationnels.

Dans l'hypothèse où un incident de sécurité avait lieu et impliquait un tiers[15] extérieur à l'organisation, la Chambre des notaires se réserve le droit d'entreprendre toutes les actions qu'elle juge appropriées, y compris des procédures judiciaires.

1.9. Entrée en vigueur et révision du cadre de sécurité des actifs informationnels

Le présent cadre de sécurité entre en vigueur lors de son adoption et peut être révisé en tout temps par le responsable de la sécurité des actifs informationnels ou à la demande du Comité d'audit et de prospectives financières de la Chambre des notaires.

Des amendements peuvent être proposés par les différents intervenants de l'organisation, lesquels devront être soumis par écrit au responsable de la sécurité des actifs informationnels.

Le présent cadre de sécurité ainsi que toute autre politique de sécurité spécifique doivent être revus au minimum tous les deux ans afin d'assurer leur pertinence compte tenu de la mission de la Chambre des notaires et des activités de ses membres.

2. Principes généraux

2.1. Organisation interne

Afin d'assurer la gestion de la sécurité de l'information au sein de l'organisation, il importe de définir la structure organisationnelle supportant la planification, l'élaboration, la mise en place et le contrôle des mesures de sécurité[16]. Le Conseil d'administration est responsable de s'assurer que cette structure organisationnelle soit définie et mise en place.

2.2. Appréciation et gestion des risques

Les mesures de sécurité mises en place s'appuient sur l'appréciation, l'analyse périodique et le traitement par la Chambre des notaires des risques relatifs à la confidentialité, à l'intégrité et à la disponibilité de l'information.

Les exigences et le processus en matière de gestion des risques[17] sont définis dans la *Politique de gestion intégrée des risques* et appliqués en tenant compte des critères d'acceptation des risques prévus par l'organisation. La Chambre des notaires s'assure ainsi que les mesures de sécurité sont déployées en fonction de l'évaluation des impacts et de la probabilité d'occurrence d'une menace[18].

Une évaluation de risques doit être effectuée avant de procéder à l'acquisition de nouveaux systèmes ou d'apporter un changement susceptible d'avoir un impact sur la sécurité de

[13] RLRQ, c. N-3.
[14] RLRQ, c. C-26.
[15] Voir Annexe 1 – Définitions.
[16] *Id.*
[17] *Id*.
[18] *Id*.

l'information. Dans tous les cas, cette évaluation doit être documentée en suivant un processus défini.

Référence: ISO27001:2013(F) 6.1; 8.2.

2.3. Attribution d'un niveau de sécurité de l'actif informationnel

L'attribution d'un niveau de sécurité[19] vise à déterminer les mesures de sécurité appropriées à chaque actif informationnel compte tenu de leur degré de sensibilité et de la cote CID[20]. Elle vise également à supporter les différents intervenants dans l'application des contrôles appropriés pour protéger les actifs informationnels contre toute divulgation, utilisation, modification ou destruction non autorisées.
La Chambre des notaires doit avoir une politique qui définit les différents niveaux de sécurité en tenant compte du *Schéma de classification*[21] et de la *Politique de gestion intégrée des risques*.
Référence: ISO27001:2013(F) A.8.2.

2.4. Acquisition, développement et maintenance des systèmes

Pour que la sécurité de l'information soit mise en œuvre efficacement, les exigences de sécurité à satisfaire lors de l'acquisition, du développement, de la mise en place et de la maintenance d'un actif informationnel doivent être déterminées. Les exigences de sécurité doivent tenir compte de l'évolution des technologies et des nouveaux enjeux.
Tout changement apporté à la Chambre des notaires, aux processus d'affaires, aux systèmes et aux moyens de traitement de l'information susceptible d'avoir une incidence sur la sécurité d'un actif informationnel doit faire l'objet d'une évaluation de risques afin d'évaluer l'impact de chaque changement proposé.
Dans le but de réduire les risques liés aux vulnérabilités techniques[22], la Chambre des notaires doit, sur une base périodique, prendre les moyens nécessaires pour découvrir les vulnérabilités, les analyser et les corriger.

Référence : ISO27001:2013(F) A.14; A.12.1.2

2.5. Gestion des incidents

Les technologies de l'information peuvent être exposées à différents types d'incidents : accidents, pannes de matériel, défaillances de sécurité, attaques informatiques, fuites d'information, etc. La mise en place d'un processus de gestion des incidents vise à traiter rapidement et efficacement tout événement qui cause ou qui pourrait causer un dommage à un intervenant, à un actif informationnel ou tout acte ou omission qui pourrait entraîner la matérialisation d'un risque.
La Chambre des notaires doit établir et définir les responsabilités et les procédures à mettre en œuvre en cas d'incident de sécurité afin de garantir une réponse rapide, efficace et pertinente. Il

[19] *Id*.
[20] *Id*.
[21] *Id*.
[22] *Id*.

est nécessaire de mettre en place une équipe capable de gérer les incidents et de coordonner les activités préalablement établies.

Référence: ISO27001:2013(F) 6.1.3; A.16.

2.6. Gestion du plan de relève

La Chambre des notaires doit mettre en œuvre un plan de relève des technologies de l'information (ci-après, « plan de relève TI »)[23] visant à réduire l'impact d'une indisponibilité d'un actif informationnel et ainsi, assurer une reprise des opérations dans les meilleurs délais. Les mesures de relève doivent être vérifiées périodiquement afin d'assurer qu'elles sont valables et efficaces.

Référence: ISO27001:2013(F) A.17.1.

2.7. Formation et sensibilisation

L'aspect humain est un élément fondamental de la protection de l'information. Il importe donc de sensibiliser le personnel à l'égard des menaces et des conséquences d'une atteinte à la sécurité afin que chacun puisse reconnaître les situations à risque et agir en conséquence.
La formation spécialisée dans des domaines liés à la sécurité de l'information est également essentielle au maintien d'un niveau de risque acceptable. Le service des ressources humaines et les gestionnaires doivent mettre en place un programme de formation et de sensibilisation à la sécurité de l'information adapté aux différents rôles de son personnel.
Tout employé doit recevoir les renseignements nécessaires à la bonne compréhension de ses responsabilités en matière de sécurité de l'information et il est de la responsabilité de l'organisation d'en informer toutes les personnes qui doivent accéder aux actifs informationnels.
À cet effet, tous les documents pertinents doivent être communiqués aux employés, incluant le présent cadre de sécurité et autres politiques afférentes. L'employé doit lire, comprendre et respecter ces documents. Il doit en outre s'engager à s'y conformer par écrit.

Référence: ISO27001:2013(F) 6.3.

3. Rôles et responsabilités

3.1. Le Conseil d'administration

Le Conseil d'administration doit approuver et prendre tous les moyens nécessaires pour mettre en œuvre le présent cadre de sécurité ainsi que les politiques et directives afférentes.

3.2. Le Comité d'audit et de prospectives financières

Ce comité recommande le cadre et ses modifications, en collaboration avec le Directeur général, au Conseil d'administration, fait la promotion d'une culture de gestion de sécurité de l'information, et assure la surveillance de la mise en œuvre du cadre pour le CA.

[23] *Id*.

3.3. Le responsable de la sécurité des actifs informationnels

Afin d'assurer la protection du public, le responsable de la sécurité des actifs informationnels doit agir à l'égard de la Chambre des notaires, de ses fournisseurs, administrateurs, partenaires, sous-traitants et mandataires de la façon suivante :

3.3.1. **Rôles**

- Définir les besoins de sécurité pour assurer la protection de l'information et les architectures de sécurité.
- Fournir un encadrement suffisant pour permettre aux propriétaires d'attribuer un niveau de sécurité aux actifs informationnels qu'ils détiennent selon les standards décrits selon le présent cadre de sécurité et le *Schéma de classification.*
- Si l'identité d'un gardien ou d'un propriétaire n'est pas clairement établie selon la structure organisationnelle, alors le responsable de la sécurité des actifs informationnels désignera les rôles.
- Rendre compte annuellement, au comité d'audit de la conformité du cadre et remise d'un rapport de conformité.

3.3.2. **Responsabilités**

- Déterminer et mettre en place les mesures de sécurité appropriées sous son contrôle, permettant d'assurer la confidentialité, l'intégrité et la disponibilité en fonction du niveau de sécurité des actifs informationnels sous son contrôle.
- Assurer que le coût des ressources allouées à la sécurité sera proportionnel à la valeur de l'actif informationnel et le niveau de risque qui y est associé.
- Sensibiliser l'ensemble des utilisateurs sur la sécurité de l'information.
- Assurer une formation adéquate en sécurité de l'information au personnel technique responsable des environnements technologiques de la Chambre des notaires.
- Définir un encadrement pour l'utilisation d'Internet, des médias sociaux et des appareils mobiles utilisés pour le travail.
- Assurer une gestion efficace des incidents de sécurité et maintenir un plan de relève TI qui implique tous les secteurs et départements basés sur les risques et les impacts.

3.4. Le responsable de la classification et de la conservation de l'information

3.4.1. **Rôles**

- Définir le niveau de sécurité associé à la confidentialité de l'information en tenant compte du *Schéma de classification* et des règles de conservation[24].

[24] *Id*.

- Définir les rôles et responsabilités attitrés à la classification de l'information et les contrôles qui y sont associés.
- Fournir un encadrement suffisant pour permettre aux propriétaires de classifier les informations qu'ils détiennent selon les standards décrits dans le présent cadre et le *Schéma de classification*.

3.4.2. **Responsabilités**

- Apporter le soutien nécessaire aux secteurs d'activité dans l'attribution d'un niveau de sécurité et dans la revue de ce classement.
- Valider tout type d'utilisation nouvelle ou différente des informations traitées dans les secteurs d'activité de la Chambre.
- Valider toutes les modifications ou les retraits des accès physiques et numériques des employés qui ont quitté l'organisation ou changé de rôle et les communiquer auprès du département des technologies de l'information (« TI »).
- Assurer la sécurité de la destruction de l'information en conformité avec les règles de conservation.

3.5. Le propriétaire de l'actif informationnel

Le propriétaire de l'actif informationnel (ci-après: « propriétaire ») est le directeur d'un secteur d'activité de la Chambre des notaires.

3.5.1. **Rôles**

- Déterminer les exigences de sécurité au sein de son secteur, lesquelles doivent être conformes au présent cadre.
- Être imputable des conséquences liées à la divulgation, de l'utilisation inappropriée, d'une mauvaise classification et de toute autre déficience des contrôles liés à la sécurité des actifs informationnels.
- Demeurer l'ultime responsable des actions exécutées à titre de propriétaire. Il ne peut se libérer de l'imputabilité de son rôle.
- Pouvoir nommer un délégué qui pourra exécuter en son nom ses responsabilités. Lorsque le propriétaire ou le délégué ne sont pas clairement identifiés ou ne sont pas disponibles, le responsable de la sécurité des actifs informationnels et le responsable de la classification et de la conservation de l'information déterminent le propriétaire ou agissent comme tel.

3.5.2. **Responsabilités**

- Désigner une personne déléguée afin d'agir en son nom à titre de propriétaire. Un tiers ou un employé non permanent ne peut être désigné à titre de délégué.
- Attribuer le code de classification et le niveau de sécurité pertinents aux actifs informationnels traités sous son secteur d'activité et assurer une revue de ce classement et du niveau de sécurité au minimum tous les deux ans.

- Identifier et assurer la mise en place des mesures de sécurité et des contrôles propres à assurer la protection de l'actif informationnel selon le niveau de sécurité attribué.
- Approuver l'attribution des droits d'accès aux actifs informationnels sous sa responsabilité en fonction des besoins requis.
- S'assurer que des précautions particulières sont prises pour protéger les informations sensibles confiées à des tiers.
- Approuver tout type d'utilisation nouvelle ou différente des informations traitées par son secteur d'activité.
- Approuver les nouveaux systèmes ou tout changement significatif aux systèmes existants qui traitent les informations, et ce, avant que ces systèmes ne soient mis en production conformément au processus de gestion des changements.
- Sensibiliser les employés sur l'importance de la sécurité et de la conformité à l'ensemble des politiques de sécurité et aux différentes lois applicables.
- Communiquer toutes les modifications ou les retraits des accès physiques et numériques des employés qui ont quitté l'organisation auprès du responsable de la classification et de la conservation de l'information.
- S'assurer d'une utilisation adéquate d'Internet, des médias sociaux et des appareils mobiles par les employés.
- S'assurer que le plan de relève TI est mis en place et soit testé de façon régulière.

3.6. Le gardien de l'actif informationnel

3.6.1. **Rôles**

- Le gardien de l'actif informationnel (ci-après : « gardien ») est une personne, morale ou physique, qui détient un ou plusieurs actifs informationnels de la Chambre des notaires pour des besoins de conservation ou de traitement, à l'exception de l'utilisateur et du propriétaire.
- Obtenir au préalable l'autorisation explicite du propriétaire pour modifier les informations en sa possession.
- Produire et communiquer au besoin au propriétaire les rapports sur les opérations des systèmes d'information en production.

3.6.2. **Responsabilités**

- Fournir les conseils et une assistance technique aux propriétaires afin que les actifs informationnels puissent être gérés selon les objectifs établis par le propriétaire.

- Protéger les actifs informationnels en leur possession, y compris la mise en œuvre des systèmes de contrôle d'accès[25] pour empêcher la divulgation inappropriée.
- Développer, documenter et tester les systèmes d'information requis dans le cadre du plan de relève TI.
- Fournir et gérer les contrôles de sécurité tels que les systèmes de sauvegardes.
- Mettre en place, contrôler et exploiter des systèmes d'information d'une manière cohérente avec le cadre de sécurité et autres politiques émis par le responsable de la sécurité des actifs informationnels.
- Obtenir les éléments d'information nécessaires en matière de sécurité de l'information afin de réaliser pleinement le rôle de gardien de l'actif informationnel.

3.7. L'utilisateur de l'actif informationnel

3.7.1. **Rôles**

- L'utilisateur de l'actif informationnel (ci-après : « utilisateur ») est une personne qui a reçu une autorisation d'accès[26] à un ou plusieurs actifs informationnels de la Chambre des notaires par un propriétaire. Les utilisateurs peuvent être des employés permanents, temporaires, administrateurs, mandataires, contractuels, consultants ou des tiers avec lesquels des arrangements spéciaux (tel que des ententes de confidentialité) ont été conclus. Tous les utilisateurs doivent être connus et autorisés par les propriétaires.

3.7.2. **Responsabilités**

- Utiliser les actifs informationnels uniquement pour les fins expressément approuvées par le gestionnaire responsable ou le propriétaire.
- Respecter toutes les mesures de sécurité définies par le propriétaire, mises en œuvre par le gardien et/ou définies par le responsable de la sécurité des actifs informationnels.
- S'abstenir de divulguer des renseignements en leur possession (sauf s'ils ont été désignés comme publics) sans l'autorisation préalable du propriétaire.
- Informer son gestionnaire responsable de toutes les situations où il croit que la sécurité d'un actif informationnel est vulnérable ou a été compromise.
- Obtenir les éléments d'informations nécessaires et un soutien en matière de sécurité des actifs informationnels afin de réaliser pleinement le rôle d'utilisateur.
- Utiliser adéquatement Internet, les médias sociaux ainsi que les appareils mobiles utilisés pour le travail conformément aux exigences de la *Directive en*

[25] *Id.*
[26] *Id*.

matière de sécurité informationnelle pour les employés de la Chambre des notaires.

- Respecter le présent cadre de sécurité et tout autre document qui s'y réfère ou qui le supporte.
- Signer une entente de confidentialité ou un serment de discrétion, selon le cas.
- Participer à toute session de formation ou à tout programme de sensibilisation mis en place par l'organisation.

3.8. Le coordonnateur de la sécurité des actifs informationnels

3.8.1. **Rôles**

- Le coordonnateur de la sécurité des actifs informationnels (ci-après « coordonnateur ») est une personne désignée par le responsable de la sécurité des actifs informationnels de la Chambre des notaires.
- Assurer la coordination entre les départements de toute question relative à la sécurité des actifs informationnels.

3.8.2. **Responsabilités**

- Définir le plan directeur[27] de la sécurité des actifs informationnels.
- Déterminer les choix technologiques, leurs critères de configuration et leur pérennité[28].
- Approuver les mécanismes et les pratiques relatifs à la sécurité des actifs informationnels.
- Fournir des conseils relatifs à la sécurité des actifs informationnels de la Chambre des notaires.
- Coordonner les mesures en matière de sécurité et approuver tout élément qui pourrait avoir un impact sur la sécurité d'un actif informationnel.
- Évaluer les informations provenant d'incidents de sécurité et émettre des recommandations quant aux actions à prendre pour le traitement de tels incidents.
- Fournir toute information utile pour l'évaluation des risques et des vulnérabilités.

Référence: ISO27001:2013(F) A.9.3

4. Contrôle d'accès aux actifs informationnels

4.1. Principe « Besoin de savoir »

L'information ne doit être divulguée qu'aux personnes qui ont besoin de cette information dans le cadre de leurs fonctions et en respectant le cadre législatif et réglementaire.

[27] *Id*.
[28] *Id.*

Référence: ISO27001:2013(F) 8.1.; A.9

4.2. Autorisation des accès

La gestion des accès doit être effectuée selon des processus et procédures formels, convenus et communiqués aux personnes concernées.

Lorsqu'un utilisateur change de fonction (incluant le licenciement, le transfert, une promotion ou un congé de longue durée), le gestionnaire responsable doit effectuer une revue de ses accès.

Une revue annuelle des comptes utilisateurs doit être réalisée par les propriétaires en collaboration avec le responsable de la sécurité des actifs informationnels.

Référence: ISO27001:2013(F) 8.1.;A.9

4.3. Contrôle des accès

Tout équipement informatique ou appareil mobile qui conserve des informations sensibles doit avoir un mécanisme actif d'authentification afin d'assurer que ces informations ne sont pas indûment divulguées, altérées, supprimées ou rendues indisponibles.

Le système de contrôle d'accès doit fonctionner par mot de passe répondant à certains critères de longueur, de qualité et de durée de vie maximale et/ou utiliser une technologie d'authentification robuste permettant l'utilisation de mots de passe dynamiques.

Les utilisateurs doivent avoir un identifiant unique et ne doivent en aucune circonstance le partager.

Les accès au système avec des comptes génériques doivent être limités, justifiés et approuvés par le responsable de la sécurité des actifs informationnels.

Référence: ISO27001:2013(F) 8.1; A.9.

5. Traitement de l'information

5.1. Partage d'information aux tiers

Sauf si elle a été désignée comme « publique », toute information doit être protégée contre toute divulgation non autorisée à des tiers. Les tiers peuvent avoir accès à l'information non classifiée comme publique seulement si un besoin a été démontré et qu'une telle divulgation a été expressément autorisée par le propriétaire ou le Comité d'accès à l'information, selon le cas.

La conclusion d'une entente de confidentialité avec les tiers doit toujours précéder la divulgation d'informations sensibles, qu'ils soient consultants, partenaires, fournisseurs, mandataires ou employés temporaires.

Référence: ISO27001:2013(F) 8.1.; A.13.2.

5.2. Manipulation d'informations sensibles des tiers

Le propriétaire ou le gardien doit s'assurer qu'un niveau de sécurité est attribué à l'information obtenue des tiers et que les mesures de sécurité appropriées sont appliquées selon le niveau attribué.

Référence: ISO27001:2013(F) 8.1; A.13.2.

5.3. Services de réparation et de maintenance

Les fournisseurs responsables de la réparation et de la maintenance des équipements informatiques qui contiennent de l'information sensible[29] (ceci inclut les fax, imprimantes et photocopieuses qui ont des zones de stockage et des journaux internes, etc.) doivent signer une entente de confidentialité à cet effet.

Référence: ISO27001:2013(F) 8.1.; A.15.

6. Communication et transmission de l'information

6.1. Transmission d'information par réseau

La transmission d'informations confidentielles sur tout réseau de communication externe de l'organisation doit être effectuée sous forme chiffrée[30] ou par une mesure de sécurité comparable. La transmission d'informations sensibles avec les notaires doit également être chiffrée et authentifiée.

Les mécanismes de sécurité acceptables et les pratiques de gestion des clés doivent être documentés. Toute connexion avec un partenaire ou un service externe doit être préalablement autorisée par le responsable de la sécurité des actifs informationnels.

Référence: ISO27001:2013(F) 8.1.; A.13.2.

7. Conservation de l'information

7.1. Supports de conservation

Les informations sensibles conservées sur des supports amovibles doivent être protégées par des mesures de sécurité appropriées. Toutes les informations sensibles contenues sur des supports amovibles qui ne sont pas chiffrées doivent être conservées dans des coffres-forts, des classeurs ou d'autres contenants qui nécessitent un mécanisme d'accès. Ceci inclut les informations qui résident sur des appareils mobiles ou toute autre technologie de conservation transportée à l'extérieur des locaux de la Chambre des notaires. Les informations sensibles conservées sur support papier doivent être conservées dans un endroit verrouillé lorsqu'elles ne sont pas utilisées.

[29] Voir Annexe 1 – Définitions.
[30] *Id.*

7.2. Livraison et transport d'un appareil mobile

Tout appareil mobile qui contient des informations sensibles et qui sort des locaux de la Chambre des notaires doit être remis personnellement au(x) destinataire(s) désigné(s).

7.3. Conservation sur serveur distant ou infonuagique

Les informations sensibles ne doivent pas résider sur des serveurs distants ou infonuagiques, sauf si préalablement autorisé par le propriétaire de l'information et après qu'une analyse de risque ait été effectuée par une personne désignée par le responsable de la sécurité des actifs informationnels.

Les exigences relatives à la conservation de l'information sensible dans l'infonuagique doivent être clairement définies. Elles doivent préciser les mesures spécifiques de sécurité requises en fonction du niveau de sécurité.

8. Destruction de l'information

Toute information de nature sensible conservée sur un appareil mobile qui n'est plus nécessaire doit être supprimée de façon permanente. Les techniques utilisées pour la suppression doivent être approuvées par le responsable de la sécurité des actifs informationnels.

Aucune information physique ou électronique ne doit être détruite si celle-ci doit être conservée selon le calendrier de conservation et/ou afin de respecter le cadre légal, contractuel ou réglementaire.

Toute destruction d'information doit être autorisée par le propriétaire de l'actif informationnel.

9. Sécurité physique et environnementale

Tous les actifs informationnels doivent être protégés par des mesures de sécurité physiques basées sur leur niveau de sécurité ainsi que sur les risques associés.

L'accès aux espaces de bureau et aux locaux informatiques contenant des informations sensibles doit être physiquement limité par un mécanisme de sécurité approprié.

L'utilisation d'un écran de veille, ou tout autre type de mesure similaire permettant de protéger l'information affichée sur les écrans contre les regards des personnes non autorisées à accéder à ces informations est obligatoire.

Référence : ISO27001:2013 (F) A.11.

ANNEXE 1 – Définitions

Actif informationnel	Les actifs informationnels visés par le présent cadre incluent non seulement l'information, mais également les équipements et les supports (papier ou numérique). Ils comprennent les données, les documents, les liens de communication internes, les sites d'hébergement, les équipements relatifs à l'exploitation, les systèmes, les applications, les appareils mobiles et tout autre équipement portable.
Appareil mobile	Tout équipement informatique ou numérique portable, incluant les ordinateurs, les supports portables, les tablettes, les téléphones intelligents, les appareils numériques, les disques durs externes, les clés USB, etc.
Autorisation des accès	Attribution de droits d'accès à un intervenant.
Chiffrement	Opération par laquelle est substitué à un texte en clair, un texte inintelligible et inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale.
Classification	Voir Schéma de classification
Confidentialité	Caractère secret, personnel ou sensible d'un actif informationnel dont l'accès et la diffusion doivent être limités aux seules personnes ou autres entités autorisées.
Contrôle des accès	Processus par lequel les données d'authentification fournies permettent l'autorisation ou le refus de l'accès demandé, qu'il soit physique ou logique.
Cote CID	Cote attribuée en fonction du niveau de risque pour la confidentialité, l'intégrité et la disponibilité de l'actif informationnel.
Cycle de vie	La période allant de la création de l'information jusqu'à sa destruction ou sa conservation permanente.
Disponibilité	Propriété d'un actif informationnel d'assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite.
Document technologique	Tout document transmis de quelque manière qu'il soit et dont le support fait appel aux technologies de l'information, au sens de la *Loi concernant le cadre juridique des technologies de l'information*.
Gestion des risques	Ensemble des activités reliées au choix, à l'évaluation et à la mise en place de mesures destinées à minimiser l'ampleur des risques de sécurité à un niveau acceptable pour l'organisation.
Incident de sécurité	Un incident lié à la sécurité de l'information découle d'un (ou plusieurs) événement indésirable ou inattendu et présentant une probabilité de

	compromettre la confidentialité, l'intégrité ou la disponibilité de l'information.
Information	Tout renseignement, qu'il soit sur support électronique ou papier.
Information sensible	Information dont l'indisponibilité ou la diffusion peut nuire à l'organisation ou à une personne. L'information sensible inclut les renseignements personnels, confidentiels, à usage restreint ou toute autre information qui n'est pas définie comme étant publique ou libre.
Intégrité	Propriété associée à l'information et à son support et qui, lors de leur utilisation, de leur transmission ou de leur accès, ne subissent aucune altération ou destruction volontaire ou accidentelle et conservent leur intégralité.
Intervenant	Tout individu, service, organisation ou tiers ayant un rôle à l'égard d'un actif informationnel dans le présent cadre de sécurité ou des responsabilités en matière de sécurité de l'information. Les intervenants comprennent son personnel, ses administrateurs, ses sous-traitants, ses fournisseurs, ses partenaires et ses mandataires.
Menace	Événement potentiel et appréhendé susceptible de porter atteinte à la sécurité de l'information.
Mesure ou contrôle de sécurité	Fonction de protection particulière, logicielle, matérielle ou procédurale qui assure, partiellement ou totalement, la protection de l'actif informationnel contre une ou plusieurs menaces informatiques, et dont la mise en œuvre vise à réduire la probabilité de survenance d'une menace ou à minimiser les impacts potentiels.
Niveau de sécurité	Attribution d'une mention qui permet de catégoriser la valeur et l'importance d'un actif informationnel et, conséquemment, le niveau de protection à lui accorder.
Organisation	Désigne la Chambre des notaires et ses intervenants.
Pérennité	Caractère de ce qui dure toujours, ou très longtemps; fait d'être durable dans le temps.
Plan de relève TI	Procédures documentées servant de guide pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une interruption, d'un incident de sécurité ou d'une force majeure.
Plan directeur	Plan de mise en œuvre des activités de sécurité de l'information requises par le cadre de sécurité et les autres politiques afférentes.
Règles de conservation	Déterminent la durée de vie et le sort (destruction, conservation ou tri) des dossiers. À chaque code du schéma de classification correspond une règle de conservation.

Risque de sécurité	Le risque est l'expression de la probabilité (niveau de certitude qu'un risque se matérialise) que des conséquences négatives ou indésirables émanent et de son impact sur l'atteinte des objectifs organisationnels, de la réalisation de la mission ainsi que sur les aspects financier, réputationnel, sécuritaire, opérationnel et de conformité.
Schéma de classification	Structure logique en forme d'arborescence servant à la classification des dossiers d'une organisation pour en faciliter le repérage et la conservation. À chaque code de classification est attribué un niveau de sécurité.
Sécurité de l'information	Terme générique désignant la protection de la confidentialité, de l'intégrité et de la disponibilité des actifs informationnels.
Signature numérique	La signature numérique (également appelée signature électronique) est un mécanisme permettant de garantir l'intégrité ou la confidentialité d'un document technologique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier.
Tiers ou tierce partie	Personne ou organisation quelconque, extérieure à la Chambre des notaires.
Vulnérabilité	Faiblesse d'un système se traduisant par une incapacité totale ou partielle de celui-ci à faire face aux menaces informatiques qui le guettent.

*À défaut de définir un terme dans une politique spécifique, les définitions du cadre de sécurité de l'information sont applicables.

ANNEXE 2 - Cadre législatif et réglementaire

Les exigences relatives à la sécurité de l'information sont présentes dans plusieurs lois, règlements et politiques applicables à la Chambre des notaires, dont notamment :

- Charte canadienne des droits et libertés (Partie I de la Loi constitutionnelle de 1982 [Annexe B de la Loi de 1982 sur le Canada, 1982, c.11 (R-U)])
- Charte des droits et libertés de la personne du Québec (RLRQ, c. C-12)
- Code civil du Québec (RLRQ, 1991, c .64), notamment les articles 36 et 37, qui portent respectivement sur le respect de la vie privée et la collecte de renseignements personnels
- Code des professions (RLRQ, c. C-26)
- Directive en matière de sécurité informationnelle pour les employés
- Guide des employés de la Chambre des notaires
- 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)
- Loi sur la protection des renseignements personnels dans le secteur privé (RLRQ, c. P-39 .1)
- Loi sur le droit d'auteur (L.R.C., 1985, c. C-42)
- Loi sur le notariat (RLRQ, c. N-3)
- Loi sur les archives (RLRQ, c. A-21 .1), en ce qui a trait aux exigences relatives à la protection et à la conservation des documents ayant une valeur patrimoniale ou archivistique
- Loi sur les marques de commerce (L.R.C., 1985, c. T-13)
- Politique de gestion intégrée des risques

Politique de la Chambre des notaires du Québec sur les documents et renseignements accessibles sans restriction