Directive de sécurité

Fournisseurs de service d'externalisation aux notaires

Préparé et sous la responsabilité du Secrétariat de l'Ordre
Approuvé le : 20 février 2014 à la séance du Comité exécutif
Mis à jour le : 18 novembre 2015 à la séance du Comité exécutif
Responsable : Danielle Gagliardi, Secrétaire de l'Ordre

Table des matières

1. Domaine d'application

La présente Directive établit des lignes directrices et des principes généraux concernant les services d'externalisation offerts aux notaires. Les objectifs présentés dans la présente Directive fournissent une orientation générale sur ce qui est communément accepté dans la gestion de la sécurité de l'information.

Les objectifs et mesures sont destinés à être mis en œuvre pour répondre aux exigences identifiées. La présente Directive représente une base commune et donne des lignes directrices pratiques pour élaborer les référentiels de sécurité, mettre en œuvre les pratiques efficaces de la gestion de la sécurité et développer un environnement de confiance dans les activités des fournisseurs.

La présente Directive de sécurité s'applique à tous les Fournisseurs de Service d'externalisation. Les mesures et contrôles applicables doivent tenir compte du service offert par le Fournisseur.

2. Termes et définitions

Pour les besoins du présent document, les mots et expressions qui suivent ont, sauf si le contexte le requiert autrement, le sens qui leur est ci-après donné et ce, indépendamment du fait qu'ils débutent ou non par une lettre majuscule :

Actif informationnel
Les actifs informationnels visés par la présente Directive comprennent les Documents technologiques, les liens de communication, les sites d'hébergement et les équipements relatifs à l'exploitation du Service d'externalisation.

Contrat de service
Signifie le contrat de fourniture de service d'externalisation aux notaires que le Fournisseur doit conclure avec le notaire selon les modalités de l'*Entente de fourniture de service d'externalisation aux notaires* conclue avec la Chambre des notaires. Le contrat de service est constitué d'un écrit contenant minimalement les dispositions de l'Annexe de cette Entente.

Document technologique
Signifie un document transmis par un notaire 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*, incluant toutes données, banques de données et métadonnées sous-jacentes qui en permettent la création. À titre d'exemple, il peut s'agir de Renseignements confidentiels, de renseignements personnels au sens des lois applicables en l'espèce, d'informations sur les clients, de courriels, de contrats ou d'ébauches d'avis juridique. Le Document technologique appartient au notaire.

Force majeure
Intervention d'un événement extérieur, irrésistible et imprévisible, telle qu'une catastrophe naturelle, et qui empêche l'exécution d'une obligation.

Fournisseur
Entreprise externe, incluant ses Partenaires, qui offre un Service d'externalisation aux notaires et qui est autorisé par la Chambre des notaires.

Incident lié à la sécurité de l'information
Un incident lié à la sécurité de l'information découle d'un ou plusieurs événements(s) de sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité du Fournisseur et de menacer la sécurité de l'information de ses clients notaires.

Interruption
Toute indisponibilité temporaire d'un Actif informationnel, à l'exception de celle résultant d'une Force majeure.

Partenaire
Signifie indistinctement tout mandataire, sous-traitant, consultant, partenaire d'affaires, revendeur, prestataire de services ou entrepreneur du Fournisseur, ainsi que les partenaires de ces derniers.

Renseignement confidentiel
Signifie une information reçue, sous quelque forme et de quelque façon que ce soit, qui concerne le Fournisseur ou tout notaire, ses employés, ses activités, ses produits ou ses procédés, sa clientèle ou ses fournisseurs et qui est désignée comme étant confidentielle ou qui doit être considérée comme étant confidentielle selon sa nature et les circonstances de la divulgation, incluant toute information sujette au secret professionnel.

Service d'externalisation
Signifie un service offert par un Fournisseur permettant à un notaire de transférer ou de confier, peu importe le moyen, en tout ou en partie, ses Documents technologiques et ses ressources informatiques physiques ou logicielles. Ce service peut notamment être la sauvegarde des Documents technologiques à distance, l'hébergement d'équipements informatiques, l'exploitation d'un système d'information ou d'applications.

3. Politique de sécurité

3.1 Politique de sécurité de l'information

« *Apporter à la sécurité de l'information une orientation* et *un soutien de la part de la direction, conformément aux exigences métier* et *aux lois et règlements en vigueur.*»

Le Fournisseur doit avoir une politique de sécurité de l'information approuvée et endossée par la direction de son entreprise. Cette politique doit être communiquée, publiée et endossée par les employés du Fournisseur.

La politique de sécurité du Fournisseur doit faire partie de sa politique générale et doit être revue périodiquement avec tous les documents auxquels elle fait référence afin de s'assurer qu'elle soit à jour et alignée aux objectifs et stratégies du Fournisseur.

Le document de politique de sécurité de l'information doit inclure au minimum:

- Une définition de la sécurité de l'information, ses objectifs et sa portée;
- Une déclaration des intentions de la direction du Fournisseur soutenant les objectifs et principes de la sécurité de l'information, en conformité avec la stratégie et les objectifs du Fournisseur;
- Une démarche de définition des objectifs de sécurité et des mesures, intégrant l'appréciation et la gestion du risque;

- Une brève explication des politiques, principes, normes et exigences en matière de conformité qui présentent une importance particulière pour le Fournisseur, à savoir les éléments suivants:
    - la conformité avec les exigences légales, réglementaires et contractuelles;
    - la gestion de la continuité de l'activité;
    - une liste des contrôles et des objectifs qu'ils sous-tendent;
    - un programme d'éducation et de sensibilisation.
- Une définition des responsabilités générales et spécifiques dans le domaine de la gestion de la sécurité de l'information, traitant en particulier de la remontée d'Incidents liés à la sécurité de l'information, ainsi que les conséquences aux manquements et sanctions applicables;
- Les références à toute documentation susceptible d'appuyer la politique et devant être respectée.

Référence: ISO27001:2013 A-5.2

4. Contrat de service

En plus des conditions prévues à l'*Entente de fourniture de service d'externalisation aux notaires*, le Fournisseur doit utiliser une entente de confidentialité et de non-divulgation, laquelle doit refléter ses besoins et ceux de ses clients notaires en matière de protection de l'information. Cette entente doit être revue périodiquement et doit minimalement adresser les points suivants:

- Une définition de l'information à protéger;
- La durée de l'entente;
- Les conséquences aux manquements et sanctions applicables à une divulgation non autorisée de l'information;
- Les droits et limites d'utilisation relative à l'information;
- Le processus général pour la notification d'un manquement à l'entente de confidentialité ou tout autre incident majeur, entre autres:
    - Panne ou mauvais fonctionnement de réseaux ou équipement;
    - Mauvais fonctionnement des systèmes;
    - Erreur humaine;
    - Non-conformité avec une politique ou directive;
    - Incident lié à la sécurité de l'information.
- Les conditions pour le transfert ou la destruction de l'information à la fin de l'entente contractuelle avec ses clients notaires;
- La conformité aux différentes lois et aux règles régissant la profession notariale ainsi que le respect des droits des personnes concernées par les Documents technologiques.

Référence: ISO27001:2013 A-15.

Tiers

« *Assurer la sécurité de l'information et des moyens de traitement de l'information consultés, opérés, communiqués ou gérés par des tiers.* »

La présente Directive s'applique aux tiers concernés et ils doivent s'y conformer. Par conséquent, si le Fournisseur sous-traite totalement ou en partie ses services à un Partenaire, c'est au Fournisseur de s'assurer que ce dernier respecte en tout point la Directive et de lui faire signer une entente à cet effet. Cette entente doit être conforme aux engagements pris par le Fournisseur avec la Chambre des notaires ainsi qu'avec ses clients notaires.

Le Fournisseur est imputable du Service d'externalisation et par conséquent, il est responsable de toutes les actions de ses Partenaires. Le Fournisseur doit déclarer ses Partenaires à la Chambre des notaires en tout temps et déclarer s'il est propriétaire ou non :

(i) des Actifs informationnels par lesquels sont transférés, conservés, copiés et généralement traités les Documents technologiques;
(ii) des locaux dans lesquels sont situés les Actifs informationnels; et
(iii) du Service d'externalisation et des solutions qui le composent et qui permettent de l'offrir.

Référence: ISO27001:2013

5. Gestion des biens

5.1 Responsabilités relatives aux Actifs informationnels

« *Mettre en place* et *maintenir une protection appropriée des biens de l'organisme.* »
Afin de maintenir la protection des Actifs informationnels relatifs à la Directive, chaque actif doit être répertorié et assigné à un propriétaire qui aura la responsabilité de maintenir les contrôles appropriés afin d'en assurer sa protection.

Les Actifs informationnels doivent demeurer au Canada et, en aucun temps, ne doivent transiter, être sauvegardés ou être traités à l'extérieur du Canada. Il est de la responsabilité du Fournisseur de s'assurer que cette obligation est respectée en tout temps.

Les Actifs informationnels doivent être utilisés, communiqués, protégés et/ou détruits en respect avec la présente Directive ainsi que les politiques applicables du Fournisseur.

Référence: ISO27001:2013

5.2 Classification des informations

« *Le fournisseur convient de garantir un niveau de protection approprié aux informations.* »

Afin de s'assurer que les Documents technologiques sont protégés adéquatement, ceux-ci doivent être classifiés en termes de confidentialité, d'intégrité et/ou de disponibilité. Un système de classification doit être mis en place et les Documents technologiques faisant l'objet du Service d'externalisation doivent être classifiés selon le plus haut niveau dans l'échelle.

Exemple :

Niveau de classification	Information
Confidentiel	Documents technologiques, etc.
Interne	Documentation des systèmes, etc.
Public	Site Web corporatif, etc.

Le Fournisseur doit individualiser et séparer les Documents technologiques de chacun de ses clients notaires afin d'en protéger la confidentialité et d'en faciliter la recherche, le transfert et la récupération lorsque requis.

Référence: ISO27001:2013

6. Sécurité liée aux ressources humaines

6.1 Avant le recrutement

« *Garantir que les salariés, contractants et utilisateurs tiers connaissent leurs responsabilités et qu'ils conviennent pour les fonctions qui leur sont attribuées à réduire le risque de vol, de fraude* ou *de mauvais usage des équipements. Il convient de sélectionner avec soin tous les postulants, contractants et utilisateurs tiers, surtout lorsqu'il s'agit de tâches critiques.* »

Les employés et Partenaires du Fournisseur, ou toutes autres personnes qu'il autorise, impliqués dans le Service d'externalisation, doivent subir une enquête de sécurité, incluant notamment, une vérification des références ainsi que des antécédents judiciaires.

Le contrat d'embauche doit spécifier les règles de confidentialité et de non-divulgation à respecter.

Référence: ISO27001:2013 A-7.1.

6.2 Pendant la durée du contrat d'embauche

Le contrat d'embauche doit spécifier que l'employé doit informer le Fournisseur de toutes situations pouvant modifier les conclusions de son enquête de sécurité. Le contrat d'embauche doit également spécifier que l'enquête de sécurité peut être renouvelée annuellement ou à la discrétion du Fournisseur.

Il est de la responsabilité du Fournisseur de faire, au minimum à tous les deux ans, une mise à jour des enquêtes de sécurité de ses employés ou des autres personnes autorisées à intervenir dans les activités de support du Service d'externalisation.

6.3 Fin ou modification de contrat d'embauche

« *Veiller à ce que les salariés, contractants et utilisateurs tiers quittent un organisme ou changent de poste selon une procédure définie.* »

Le Fournisseur doit avoir une procédure formelle pour la restitution des biens, la modification ou la suppression des droits d'accès aux moyens de traitement de l'information lors de la fin ou de la modification du contrat d'embauche d'un de ses employés.

Référence: ISO27001:2013 A-7.3.

7. Sécurité physique et environnementale

7.1 Zones sécurisées

« *Empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux et les informations de l'organisme.* »

Les Actifs informationnels doivent être protégés par des mesures de sécurité physique permettant le contrôle des accès aux employés autorisés seulement.

Les exigences en matière de sécurité physique pour la salle d'hébergement sont:

- Les murs doivent être renforcés allant du vrai plancher au vrai plafond;
- Les portes d'accès ou de sortie d'urgence doivent être pleines;
- Pour une salle d'hébergement située à un niveau inférieur au troisième étage, les vitres extérieures devraient être obstruées par un grillage ou tout autre moyen dissuasif;
- Un système de contrôle d'accès ou poste de garde avec vérification d'identité doit être en place;
- Un registre des accès (nom, date, heure d'entrée et de sortie) doit être en place;
- La salle d'hébergement doit être pourvue d'un système de surveillance ou, lorsque la surveillance n'est pas possible, d'un système de détection d'intrusion actif en l'absence d'une personne autorisée;
- L'accès à la salle d'hébergement ne doit être possible qu'à partir d'une autre zone à accès contrôlé et non depuis une zone à accès public;
- Le personnel non autorisé à la salle d'hébergement doit être accompagné d'un garde ou d'un membre du personnel autorisé.

Référence: ISO27001:2013 A-11

7.2 Sécurité du matériel

« *Empêcher la perte, l'endommagement, le vol ou la compromission des biens et l'interruption des activités de l'organisme.* »

Les exigences en matière de sécurité matérielle applicables sont:

Salle d'hébergement

- La salle d'hébergement doit être dotée d'une alimentation électrique d'appoint conforme aux normes de protection contre les incendies;
- La climatisation de la salle d'hébergement doit être suffisante aux besoins des équipements s'y trouvant et conforme aux normes de protection contre les incendies;
- La température et l'humidité doivent être contrôlées;
- Si l'information n'est pas chiffrée, le câblage réseau ne devrait pas passer dans une zone publique.
- Les mesures de protection contre les incendies doivent être égales ou supérieures aux meilleures pratiques de l'industrie du Service d'externalisation.

Cabinets

- Les cabinets contenant les serveurs hébergeant des Renseignements confidentiels doivent être verrouillés;
- L'accès aux cabinets doit être restreint au personnel autorisé seulement.

Référence: ISO27001:2013 A-11

8. Gestion de l'exploitation et des télécommunications

8.1 Procédures et responsabilités liées à l'exploitation

« *Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.* »

Tous les changements doivent être préalablement testés et approuvés avant d'être portés sur l'environnement de production.

Référence: ISO27001:2013 A-12

8.2 Sauvegarde

« *Maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information.* »

La sauvegarde des Documents technologiques doit être faite quotidiennement et doit être chiffrée. Des tests de restauration concluants doivent être exécutés au minimum une fois par mois.

La sauvegarde des Documents technologiques ne peut être faite à l'extérieur du Canada.

Dans le cas d'un Service d'externalisation d'hébergement d'infrastructure ou d'applications, une copie de sauvegarde des Documents technologiques doit être entreposée à l'extérieur de l'immeuble du Fournisseur, mais en territoire canadien, au moins une fois par semaine, dans des locaux répondant aux exigences de sécurité décrites à la présente Directive.

Les archives et les sauvegardes, peu importe le support, doivent faire l'objet d'une procédure claire quant à leur identification et manipulation. Cette information est importante et confidentielle et ne devrait être manipulée, détenue et/ou détruite que par le personnel ou les parties autorisées.

Le Fournisseur doit assurer la pérennité des Documents technologiques :

- Mettre en place des alertes relatives aux formats d'encodage des Documents technologiques afin d'aviser la personne à l'origine du dépôt de l'obsolescence du format;
- Assurer la disponibilité et l'accessibilité des Documents technologiques conformément à l'*Entente de fourniture de service d'externalisation aux notaires* conclue avec la Chambre des notaires;
- Assurer la pérennité des technologies supportant les Documents technologiques pendant toute la durée de conservation prévue pour ces derniers.

Référence: ISO27001:2013 A-12

8.3 Gestion de la sécurité des réseaux

« *Assurer la protection des informations sur les réseaux et la protection de l'infrastructure sur laquelle ils s'appuient.*»

Le Fournisseur doit utiliser un coupe-feu. Cependant, comme ce coupe-feu sécurise uniquement la communication nécessaire entre l'Internet et le serveur d'applications, et entre le serveur d'applications et le serveur de base de données, un système de prévention des intrusions doit servir de complément de protection logique au coupe-feu.

L'architecture doit être en mode trois tiers. De plus, la base de données et le serveur d'applications doivent être sur deux segments distincts.

La communication entre les consoles de gestion et les serveurs doit être chiffrée, à moins que la console soit directement connectée aux serveurs. Si elle est initiée de l'externe, la communication doit passer par un réseau privé virtuel (VPN).

Les réseaux de développement et de test ne doivent pas être dans le même sous-réseau IP («*Internet Protocol*») que les environnements de préproduction et de production.

Référence: ISO27001:2013 A-12

8.4 Manipulation des supports

« *Empêcher la divulgation, la modification, le retrait* ou *la destruction non autorisée de biens* et *l'interruption des activités de l'organisme.* »

Les médias, ou tout autre système ayant servi à offrir le Service d'externalisation ou ayant contenu les Documents technologiques, qui ne servent plus à fournir le Service d'externalisation doivent être détruits de façon sécuritaire. Par exemple, les médias doivent être détruits physiquement ou par écriture multiple avec confirmation d'exécution. Le but est de s'assurer que les Documents technologiques qui y étaient contenus ne sont plus récupérables, lisibles ou utilisables.

Référence: ISO27001:2013 A-12

8.5 Échange des informations

« *Maintenir la sécurité des informations et des logiciels échangés au sein de l'organisme et avec une entité extérieure.*»

L'échange électronique d'information confidentielle doit être sécurisé, que ce soit entre le Fournisseur et une tierce partie, entre le Fournisseur et le notaire ou entre le Fournisseur et la Chambre des notaires. Dans le cas de médias contenant des Documents technologiques, le Fournisseur doit s'assurer d'utiliser un algorithme reconnu comme fiable pour le chiffrement des Documents technologiques et d'utiliser un transporteur offrant des garanties de sécurité et permettant une traçabilité des médias.

Si une synchronisation ou une sauvegarde des Documents technologiques est effectuée entre le serveur de base de données et un autre serveur, la communication doit être chiffrée si les Documents technologiques ne le sont pas.

Référence: ISO27001:2013 A-12.

8.6 Service de commerce électronique

« *Assurer la sécurité des services de commerce électronique, tout comme leur utilisation sécurisée.* »

Le Fournisseur doit assurer la protection contre les accès non autorisés. Ainsi, tout utilisateur doit être adéquatement authentifié (par exemple à l'aide d'un code utilisateur et mot de passe individuel) avant d'être autorisé à consulter ou modifier les Documents technologiques.

Référence: ISO27001:2013 A-12.

8.7 Surveillance

« Détecter les traitements non autorisés de l'information. »

La date et l'heure des serveurs et des équipements réseau doivent être synchronisées avec un serveur de temps.

Le Fournisseur doit conserver et protéger les journaux d'accès, d'événements de sécurité et d'activités sur les Documents technologiques pour une période d'au moins 12 mois. Les journaux doivent être analysés régulièrement afin de détecter toute anomalie sur les Actifs informationnels qui permettent d'offrir le Service d'externalisation.

Référence: ISO27001:2013 A-12, ISO27018:2014 12.4.2.

9. Contrôle d'accès du personnel du Fournisseur

9.1 Gestion de l'accès utilisateur

« *Maîtriser l'accès utilisateur par le biais d'autorisations* et *empêcher les accès non autorisés aux systèmes d'information.* »

Une procédure d'enregistrement et de révocation des droits d'accès des comptes utilisateurs doit être en place et revue annuellement. Cette procédure doit respecter les points suivants:

- Un identifiant unique pour chaque utilisateur.
- Maintenir à jour une liste des utilisateurs.
- Seulement les privilèges nécessaires doivent être associés au compte de l'utilisateur ou de l'administrateur.

Une procédure de contrôle d'accès doit être mise en place et doit respecter les points suivants :

- Vérification de l'identité de l'utilisateur avant de lui donner un nouveau mot de passe, que ce soit temporaire ou pour un remplacement.
- Les mots de passe temporaires doivent être transmis d'une manière sécuritaire.
- Les mots de passe doivent respecter les meilleures pratiques au niveau de la complexité, de la fréquence de changement et l'historique :
    - Utiliser un mot de passe d'au moins 8 caractères, composé de lettres, chiffres, d'au moins un caractère spécial (#1$%&), d'une minuscule et d'une majuscule.
    - Éviter d'utiliser un mot de dictionnaire ou un mot qui ressemble au nom du Fournisseur, du service, du logiciel, du système ou de l'employé.
- Le verrouillage (temporaire ou permanent) des comptes doit être activé après un nombre défini de tentatives infructueuses.
- Un système doit engendrer une déconnexion automatique des sessions inactives après un délai défini.
- L'accès aux serveurs et aux équipements réseau doit être contrôlé au minimum par un identifiant et un mot de passe.
- Les identifiants génériques ne doivent être utilisés que lorsqu'il n'y a aucune alternative.
- Ne pas permettre à un utilisateur d'ouvrir une session de travail sous l'identifiant d'un autre utilisateur, à moins d'avoir été formellement autorisé par le supérieur de ce dernier. Dans ce dernier cas, cette action doit être enregistrée dans un registre.
- L'écran de veille avec mot de passe doit être activé, permettant de verrouiller automatiquement le poste de travail ou le serveur lorsqu'il est hors d'usage pendant une période maximale de dix (10) minutes ou permettant de verrouiller l'ordinateur manuellement.
- Révoquer immédiatement les droits d'utilisation d'un administrateur lors d'un départ ou d'un Incident lié à la sécurité de l'information où sa responsabilité est en cause.

9.2 Responsabilités utilisateurs

« *Empêcher les accès utilisateurs non habilités et la compromission ou le vol d'informations et de moyens de traitement de l'information.* »

Les utilisateurs, employés du Fournisseur, doivent:

- Utiliser les systèmes en respect des règles et politiques en vigueur.

- Ne jamais laisser sans surveillance des Documents technologiques qui ne sont pas protégés (ex. : sans chiffrement), quel que soit le support ou le média sur lequel ils se trouvent.

Référence: ISO27001:2013 A-9.

9.3 Contrôle d'accès au réseau

« *Empêcher les accès non autorisés aux services disponibles sur le réseau.* »

Les connexions à distance aux réseaux de production et de relève doivent être effectuées par Réseau Privé Virtuel (« VPN ») ou un canal sécurisé.

Aucun accès sans-fil non protégé ne doit être possible directement dans les environnements de production et de relève. Au minimum, le chiffrement WPA2 est requis.

Une authentification est requise pour se connecter sur les ports de diagnostics ou de configuration suivant les meilleures pratiques.

Référence : ISO27001:2013 A-9.

9.4 Contrôle d'accès aux applications et à l'information

« *Empêcher les accès non autorisés aux informations stockées dans les applications.* »

Les infrastructures permettant d'offrir le Service d'externalisation doivent être logiquement isolées de tous les autres services pouvant être offerts par le Fournisseur.

Une authentification individuelle est requise pour accéder aux systèmes et aux Documents technologiques.

Référence: ISO27001:2013 A-9.

9.5 Informatique mobile et télétravail

« *Garantir la sécurité de l'information lors de l'utilisation d'appareils informatiques mobiles* et *d'équipements de télétravail.* »

Le chiffrement des Documents technologiques est requis sur tous les équipements mobiles. Ce chiffrement doit être effectué en utilisant un algorithme reconnu comme fiable.

Référence: ISO27001:2013 A-9.

10. Développement et maintenance des systèmes

10.1 Bon fonctionnement des applications

« *Empêcher toute erreur, perte, modification non autorisée ou tout mauvais usage des informations dans les applications.* »

Des validations des paramètres d'entrée doivent être effectuées afin d'éviter l'injection de code (valeur hors limite, caractères spéciaux, requêtes SQL (« *Structured Query Language* »), chaîne de caractères volumineuse, etc.). Voir également la section 10.4.

Référence: ISO27001:2013

10.2 Mesures cryptographiques

«*Protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des moyens cryptographiques.*»

Les Documents technologiques entreposés chez un Fournisseur doivent être chiffrés, à moins que d'autres mesures de protection équivalentes ou supérieures ne soient mises en place.

Les Documents technologiques doivent être chiffrés avant de quitter tout système informatique du Fournisseur ou du notaire. Si le document technologique lui-même n'est pas chiffré, un tunnel chiffré doit être utilisé entre les systèmes informatiques pour sécuriser les Documents technologiques en transit.

L'algorithme de chiffrement utilisé doit être conforme aux meilleures pratiques sur le marché permettant d'assurer un bon niveau de protection. Toutefois, une méthode de recouvrement de la clé de chiffrement doit permettre de rendre les Documents technologiques accessibles au notaire, à la Chambre des notaires ou à une personne autorisée en vertu de la loi, notamment un syndic de la Chambre des notaires.

Référence: ISO27001:2013 A-10.

10.3 Sécurité des fichiers système

« *Garantir la sécurité des fichiers système.* »

Tous les changements doivent être préalablement testés et approuvés avant d'être portés sur l'environnement de production.

Les serveurs et autres composantes critiques supportant le Service d'externalisation doivent avoir fait l'objet d'un durcissement (« *hardening* ») de leur sécurité avant d'être mis en production.

Référence: ISO27001:2013

10.4 Sécurité en matière de développement et d'assistance technique

Les Renseignements confidentiels ne doivent jamais être copiés dans les environnements de développement, de test et/ou de pré-production, à moins que ces environnements offrent des mesures de sécurité comparables à celles de l'environnement de production ou que les Documents technologiques aient été rendus anonymes.

Référence: ISO27001:2013 A-14.2

10.5 Gestion des vulnérabilités techniques

« *Réduire les risques liés à l'exploitation des vulnérabilités techniques ayant fait l'objet d'une publication.* »

Les systèmes et les applications doivent être configurés afin d'en assurer la sécurité. Uniquement les services ou les modules nécessaires doivent être actifs. Les correctifs de sécurité, tant applicatifs que systèmes, doivent être testés et appliqués dans un délai raisonnable afin d'assurer la sécurité générale des Actifs informationnels dans un délai raisonnable.

Référence: 1SO27001:2013 A-14.2

11. Gestion des Incidents liés à la sécurité de l'information

11.1 Signalement des événements et des failles liés à la sécurité de l'information

« Garantir que le mode de notification des événements et failles liés à la sécurité de l'information permette la mise en œuvre d'une action corrective, dans les meilleurs délais. »

Le Fournisseur doit mettre en place des mesures de sécurité efficaces pour détecter les Incidents liés à la sécurité de l'information pouvant avoir un impact sur la confidentialité, l'intégrité ou la disponibilité des Documents technologiques ou du Service d'externalisation. Tout Incident lié à la sécurité de l'information détecté doit être inscrit dans un registre et rapporté aux notaires concernés et à la Chambre des notaires dans les 48 heures (plus spécifiquement au secrétaire de l'Ordre), notamment dans les cas suivants :

- Une perte ou un vol de Documents technologiques découlant du Service d'externalisation, que cette menace se produise du côté du client-notaire ou du Fournisseur (si celui-ci en est avisé).
- Une panne prolongée des systèmes servant à offrir le Service d'externalisation.
- Une compromission (ex. : piratage) des systèmes du Fournisseur.

À cet effet, le Fournisseur doit avoir une politique et un processus clairs pour la gestion des Incidents liés à la sécurité de l'information au sein de son organisation et pour la notification de ces derniers. Le Fournisseur doit conserver tous les Documents technologiques et les preuves relatives aux Incidents liés à la sécurité de l'information pendant cinq (5) ans (incluant le nom des témoins, la période, les Documents technologiques et clients affectés). Il doit également assurer l'intégrité de ces preuves.

Référence: ISO27001:2013 A-16, ISO27002:2013, ISO27018:2014 s.16

12. Gestion du plan de continuité de l'activité

12.1 Aspects de la sécurité en matière de gestion de la continuité de l'activité

« *Neutraliser les interruptions des activités de l'organisme, protéger les processus métier cruciaux des effets causés par les principales défaillances des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dons les meilleurs délais.* »

Un processus de continuité des affaires du Fournisseur doit être implanté afin de minimiser les impacts d'une indisponibilité des Actifs informationnels ou du Service d'externalisation à un niveau acceptable par la Chambre des notaires. Ces indisponibilités pourraient être causées, par exemple, par une catastrophe naturelle, un accident, un Incident lié à la sécurité de l'information, un bris d'équipement ou un acte délibéré.

Le processus de continuité des affaires doit inclure les points suivants:

- Identification des rôles et responsabilités.
- Identification des procédures:
    - Procédure d'urgence;
    - Procédure de recouvrement;
    - Procédure de restauration;
    - Procédure opérationnelle temporaire;
    - Procédure de reprise des opérations normales.
- Identification du niveau acceptable pour l'indisponibilité du Service d'externalisation. À cet effet, le Fournisseur doit assurer la disponibilité des Actifs informationnels en moins

de 4 heures lorsque survient une Interruption du Service d'externalisation. Dans les cas de Force majeure, le Fournisseur doit rendre les Actifs informationnels disponibles en moins de 72 heures.
- Documentation et mise en place des procédures de recouvrement et de restauration du Service d'externalisation ou des Documents technologiques.
- Inventaire des Actifs informationnels (serveurs, logiciels, licences, etc.)
- Tests documentés et mise à jour du plan de continuité des affaires au moins une fois par année.

Une copie du plan de continuité des affaires doit être conservée aux sites de relève et une autre au site de production. Le niveau de sécurité concernant l'accès aux copies du plan de continuité des affaires doit être le même que celui pour l'accès au plan original. En tout temps, les copies doivent être conformes au plan original.

Les sites de relève doivent être situés à au moins 20 kilomètres du site de production.

Référence: IS027001:2013 A-17

13. Remise des Actifs informationnels aux notaires

Lorsque le Fournisseur doit effectuer une remise des Actifs informationnels qui lui ont été confiés, cette remise doit en comprendre la totalité et s'effectuer de façon sécurisée. Pour ce faire, le Fournisseur peut soit chiffrer les Documents technologiques ou utiliser un moyen de transfert sécurisé, tel que SFTP ou FTPS. Le Fournisseur doit ensuite détruire les Documents technologiques sur ses équipements conformément aux dispositions pertinentes de l'Entente de fourniture de service d'externalisation aux notaires.

14. Destruction sécuritaire des Documents technologiques

Lorsque la destruction des Documents technologiques est requise, le Fournisseur doit les détruire de façon sécuritaire et permanente. Le Fournisseur doit produire au notaire ou à la Chambre une déclaration écrite à cet effet, sur simple demande du notaire ou de la Chambre selon le cas, et indiquer le procédé utilisé pour la destruction.

15. Signature numérique des notaires

Si le Fournisseur utilise la signature numérique du notaire dans le cadre du Service d'externalisation, cette utilisation doit être conforme aux directives de Solutions Notarius inc. et/ou Notarius - technologies et systèmes d'information notariale inc. sur le sujet.