IMPLANTATION D'UN SYSTÈME DE GESTION ÉLECTRONIQUE :
SPÉCIFICATIONS TECHNIQUES À L'INTENTION DES AGENCES ET COURTIERS À LEUR COMPTE

IMPORTANT

L'OACIQ se réserve le droit de modifier ses exigences en fonction de l'évolution des domaines technologique et juridique.

1. SAUVEGARDE DE L'INFORMATION

NOTE EXPLICATIVE :

La préservation de l'information concerne notamment deux aspects qu'il faut bien distinguer :

- **Stockage** : Enregistrement de l'information dans un but de réutilisation future. Le stockage doit rendre l'information disponible aux utilisateurs autorisés pour sa réutilisation.
- **Sauvegarde** (back-up): La sauvegarde consiste à dupliquer et mettre en sécurité les données du système dans le but de restaurer l'information du système suite à un incident de rupture d'équipement (bris d'un disque du système) ou à une action de modification des données accidentelle ou non désirée.

1.1. Contenu de la sauvegarde

Le concepteur doit décrire :

- ✓ les fichiers qui sont inclus dans la procédure de sauvegarde;
- ✓ l'exhaustivité du contenu sauvegardé;
- ✓ le système de stockage des données (un système de fichiers ou une base de données, ou les deux).

Exemples :

- ✓ Les informations du système sont sauvegardées dans une base de données. Toute la base de données utilisée par la solution est sauvegardée, y compris les données de gestion du système;
- ✓ Les informations du système sont sauvegardées dans des fichiers et non pas dans une base de données. Seuls les dossiers des courtiers actifs sont sauvegardés.

1.2. Unité de stockage

Le concepteur doit indiquer le type d'unités de stockage qui est utilisé pour la sauvegarde des fichiers.

Exemples :

- ✓ Disque externe en local;
- ✓ Disque externe sur réseau;
- ✓ Sauvegarde envoyée vers une entreprise spécialisée dans la sauvegarde de données;
- ✓ Bande magnétique.

1.3. Procédure

Le concepteur doit décrire la procédure de sauvegarde en indiquant :

- ✓ la stratégie de sauvegarde : utilisation de sauvegardes complètes, incrémentales, différentielles;
- ✓ la fréquence et la période de conservation des différents types de sauvegarde;
- ✓ les techniques de sauvegarde quotidienne, hebdomadaire, mensuelle et annuelle, s'il y a lieu.

Exemples :

- ✓ Une sauvegarde complète de la base de données est effectuée toutes les nuits. Cette copie est ensuite envoyée vers une entreprise spécialisée en sauvegarde et est conservée pendant deux mois.
- ✓ Une sauvegarde complète est faite toutes les semaines le lundi à minuit (conservée 2 semaines) et une sauvegarde différentielle est faite tous les jours à minuit (conservée 2 semaines).
- ✓ Une sauvegarde complète est faite tous les jours à minuit (conservée pendant 1 mois sur disque dur externe local et envoyée quotidiennement au service de sauvegarde externe pour conservation d'une semaine). Une sauvegarde incrémentale est effectuée toutes les heures (conservée 2 jours sur disque dur réseau).

1.4. Lieu d'entreposage

Le concepteur doit indiquer le lieu d'entreposage des copies de sauvegarde. À noter que l'OACIQ autorise les lieux d'entreposage au Canada et aux États-Unis, puisque les normes en matière de protection des renseignements personnels y sont reconnues et sûres. Cependant, le Canada est à privilégier, puisqu'en tout temps et de façon régulière, l'OACIQ réévalue la pertinence de permettre ou de retirer l'autorisation des lieux d'entreposage en dehors du Canada.

Par ailleurs, les copies de sauvegarde doivent être entreposées à l'extérieur du lieu de résidence de l'information source, dans un endroit sécurisé et à l'abri des intempéries et des détériorations.

Exemples :

- ✓ La sauvegarde est faite sur un disque dur réseau situé sur un site extérieur au site d'opération du système; le local de serveurs abritant ces disques durs est sécurisé et son accès n'est possible qu'aux personnes responsables des sauvegardes;
- ✓ La sauvegarde étant faite sur des bandes magnétiques dans les locaux d'opérations du système, elles sont quotidiennement apportées dans un coffre ignifugé dans un local externe à […].

1.5. Récupération

Le concepteur doit expliquer la procédure de récupération des fichiers en cas de bris majeur, ainsi que le temps estimé de récupération.

1.6. Système de redondance

Le concepteur doit indiquer la stratégie de redondance mise en place. En l'absence d'une stratégie ou d'un système de redondance, le concepteur doit indiquer :

- ✓ La période maximum pendant laquelle il peut y avoir perte d'information en relation avec la stratégie de sauvegarde.
- ✓ Le processus qu'il entend mettre en place pour se prémunir contre la perte d'information advenant un bris d'équipement entre deux sauvegardes.

1.7. Registre d'exécution

Le concepteur doit pouvoir présenter un registre d'exécution (ou journal d'exécution) qui indique les divers paramètres d'exécution des sauvegardes. Le registre doit contenir au minimum les éléments suivants :

- ✓ la date d'exécution;
- ✓ le type de sauvegarde; et
- ✓ les anomalies, s'il y a lieu.

2. INTÉGRITÉ DE L'INFORMATION

NOTE EXPLICATIVE :
L'intégrité d'un document résulte de deux éléments :

- Lorsqu'il y a possibilité de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité.
- Lorsque le support qui porte cette information lui procure la stabilité et la pérennité voulue.

Les critères ci-dessous visent à s'assurer que ces deux éléments soient respectés.

2.1. Preuve d'intégrité

Le concepteur doit décrire les mécanismes assurant l'intégrité de l'information. Celui-ci doit prouver hors de tout doute raisonnable que l'information ne peut être altérée frauduleusement ou par inadvertance.

2.2. Journalisation des opérations

Le concepteur doit démontrer la procédure de suivi des opérations effectuées dans le système et :

- ✓ lister toutes les actions et les groupes d'utilisateurs les effectuant qui déclenchent une entrée dans le journal des opérations.
- ✓ fournir une copie du journal des opérations, ainsi que le détail d'une entrée du journal.

Le journal des opérations doit :

- ✓ indiquer le nom de la personne exécutant l'opération, l'heure et la date à laquelle l'opération a été exécutée et la donnée affectée;
- ✓ ne pas pouvoir être altéré;
- ✓ être conservé aussi longtemps que les documents;
- ✓ être accessible par l'agence.

3. SÉCURITÉ D'ACCÈS

NOTE EXPLICATIVE :

- Confidentialité : seul le destinataire (ou le possesseur) légitime d'un document pourra en avoir une vision intelligible
- Authentification : lors de l'envoi d'un document ou lors de la connexion à un système, on connaît sûrement l'identité de l'émetteur ou l'identité de l'utilisateur qui s'est connecté.
- Intégrité : on a la garantie qu'un document n'a pas été altéré, accidentellement ou intentionnellement.
- Non-répudiation : l'auteur d'un document ne peut pas renier son œuvre.

Les critères ci-dessous visent à s'assurer que ces quatre concepts sont respectés.

3.1. Attribution des accès

Le concepteur doit indiquer les outils de gestion des accès :

- ✓ le nom du groupe d'utilisateurs ou de l'utilisateur qui accorde les autorisations aux autres utilisateurs;
- ✓ les mécanismes garantissant l'intimité d'accès des individus (modification des mots de passe).

3.2. Groupe d'utilisateurs

Le concepteur doit indiquer :

- ✓ les groupes d'utilisateurs qui ont accès au système, incluant l'administrateur du système (fournisseur);
- ✓ les utilisateurs qui font partie de ces groupes;
- ✓ les permissions et les accès de ces groupes :
  - les fonctionnalités auxquelles chacun des groupes a accès (ex. : consultation, édition, suppression, transmission, etc.);
  - les données que ces différents groupes peuvent consulter, modifier, ajouter, supprimer, transmettre;
    - le détail du profil établi pour les inspecteurs de l'OACIQ, soit l'accès à toutes les données en lecture seule et, le cas échéant, l'accès aux registres, à la comptabilité en fidéicommis et à la comptabilité générale, et ce, comme prescrit par le *Règlement sur les dossiers, livres et registres, la comptabilité en fidéicommis et l'inspection des courtiers et des agences* dans le cas où le système offre de façon électronique ces composantes. L'OACIQ doit pouvoir imprimer et télécharger ces documents.

3.3. Maintien de la confidentialité d'accès

Le concepteur doit indiquer les mécanismes permettant d'assurer le maintien de la confidentialité d'accès des utilisateurs, particulièrement dans le cas où l'application est accessible par les clients et qu'une authentification électronique est requise.

3.4. Résiliation des droits d'accès

Le concepteur doit décrire les processus permettant d'interrompre l'accès au système des utilisateurs, quelle qu'en soit la raison : changement d'agence, fin de l'abonnement au service, etc. Le processus doit permettre de reconnaître à temps la résiliation de l'accès et d'interrompre immédiatement l'accès.

3.5. Gestion des accès

3.5.1. Système via Internet

Le concepteur doit démontrer que les mécanismes d'authentification au système respectent le standard minimal de niveau 2. Ce niveau nécessite l'attribution d'un code utilisateur et d'un mot de passe après présentation de pièces justificatives, soit en personne ou autrement.

3.5.2. Système en réseau

L'agence doit démontrer que des mécanismes de contrôle d'accès au lieu physique à partir duquel la solution est accessible ont été mis en place.

4. TYPES DE CONTENU DU SYSTÈME

4.1. Gestion des registres et dossiers prescrits par le *Règlement sur les dossiers, livres et registres, la comptabilité en fidéicommis et l'inspection des courtiers et des agences*

Le système doit permettre de gérer, **tous ou certains** registres et dossiers prescrits par le *Règlement*. Le concepteur doit identifier les types de registres ou de dossiers pris en charge par le système et décrire les mécanismes qui permettent de garantir l'inclusion des documents selon le contexte d'évolution du dossier et la dépendance des documents entre eux :

- ✓ Selon le type de dossier (dossier de contrat de courtage ou dossier de transaction), celui-ci ne pourra être complété sans que les documents et informations obligatoires ne s'y retrouvent.
- ✓ Le système doit permettre de rattacher à un dossier tout type de document nécessaire à la complétion de ce dossier.
- ✓ En cours d'évolution d'un dossier, certains documents deviennent obligatoires. Ils doivent donc être obligatoires à certains moments, selon le statut du dossier.

Exemples :

- ✓ Un dossier d'inscription doit obligatoirement inclure un contrat de courtage.
- ✓ La vente d'une copropriété doit obligatoirement contenir l'entente de copropriété.
- ✓ Lors du dépôt d'une promesse d'achat acceptée et prévoyant un acompte, la copie du chèque et le reçu en fidéicommis doivent être ajoutés au dossier.
- ✓ Etc.

5. ÉCHANGE D'INFORMATION

5.1. Description de l'outil d'échange d'information

Le concepteur doit présenter l'outil d'échange d'information inclus dans la solution :

- ✓ types d'informations pouvant être échangées;
- ✓ mode d'échange d'information;
- ✓ niveau d'automatisation des échanges.

Le concepteur doit fournir une copie d'écran pour illustrer la fonctionnalité d'échange d'information.

N. B. En raison de la nature des documents, qui peuvent contenir des renseignements personnels, confidentiels ou de nature commerciale ou financière, l'OACIQ favorise un mode de communication sécuritaire, notamment le courriel sécurisé, un site sécurisé FTP ou autre.

Exemple :

- ✓ L'outil permet aux courtiers d'envoyer, par courriel seulement, un ou l'ensemble des documents contenus dans un dossier.

5.2. Gestion des accès à l'outil d'échange d'information

Le concepteur doit détailler le processus de sécurité et de limitation d'accès au système d'échange d'information :

- ✓ nom des groupes d'utilisateurs qui peuvent utiliser l'outil d'échange d'information;
- ✓ types d'informations que ces utilisateurs peuvent échanger;
- ✓ mode de définition des rôles et responsabilités des utilisateurs de l'application d'échange d'information.

Exemples :

- ✓ Seuls les utilisateurs du groupe « Courtiers » peuvent utiliser l'outil d'échange d'information, et ils ne peuvent envoyer que leurs propres dossiers ou les documents contenus dans leurs dossiers.
- ✓ Les utilisateurs du groupe « Assistant administratif » ne peuvent qu'envoyer les dossiers (ou documents d'un dossier) appartenant aux utilisateurs du groupe « Courtier » auxquels ils sont rattachés.

5.3. Historique

Le concepteur doit décrire les mécanismes de journalisation des transactions d'échange et :

- ✓ lister toutes les actions d'envoi et les groupes d'utilisateurs les effectuant qui déclenchent une entrée dans le journal des transactions d'échange;
- ✓ fournir une copie du journal des transactions d'échange, ainsi que du détail d'une entrée du journal de transactions d'échange.

Le journal doit contenir minimalement la date, l'heure du début de l'échange et le destinataire.

6. AUTHENTIFICATION DES DOCUMENTS

6.1. Numérisation des documents

6.1.1. Logiciel de numérisation intégrée au système

Le concepteur doit décrire le processus de numérisation et présenter :

- ✓ la procédure de numérisation indiquant notamment les étapes à réaliser par les utilisateurs, les appareils utilisés et les paramètres à appliquer;
- ✓ les mécanismes de transfert par lesquels les fichiers sont intégrés dans la solution GED.

Le concepteur doit démontrer que la numérisation respecte les exigences de la Loi sur le cadre juridique des technologies de l'information . Pour plus de détails, voir les articles « Numérisation des dossiers : avant de détruire, documentez-vous! », « La gestion électronique des documents : la numérisation, accordez-y de l'importance », « La gestion électronique des documents : quelques écueils à éviter » et « Le contrôle de qualité : une étape à ne pas négliger » ainsi que le guide « Numérisation : visez la qualité et documentez-vous! », disponibles sur le site Web de l'OACIQ.

L'OACIQ reconnaît les paramètres de numérisation recommandés par Bibliothèque et Archives Nationales du Québec (BANQ), soit une résolution d'image de **300 dpi** (ppp).

6.1.2. Logiciel de numérisation non intégrée au système

Le concepteur doit indiquer :

- ✓ comment les documents seront ajoutés à la solution;
- ✓ la nature des liens entre le système de numérisation et le système de GED, s'il y a lieu;
- ✓ comment il envisage de diffuser de bonnes pratiques de numérisation auprès de ses clients, par exemple en fournissant une procédure de numérisation ou un modèle de procédure;

6.2. Authentification du document

Le concepteur doit indiquer la procédure mise en place pour s'assurer que :

- ✓ l'information est accessible uniquement par les personnes autorisées;
- ✓ les métadonnées incluent l'auteur du document;
- ✓ le document n'a pas été altéré accidentellement ou intentionnellement;
- ✓ chaque opération réalisée sur le document est enregistrée automatiquement, de sorte qu'une personne ne peut nier avoir exécuté une modification.

6.3. Signature manuscrite :

Le concepteur doit prouver que tous les documents qui sont signés de façon manuscrite ne peuvent être altérés à partir du moment où ils sont déposés dans le système de GED.

Exemple :

- ✓ Les documents signés doivent obligatoirement être en format PDF. Ainsi, ces documents ne peuvent être altérés accidentellement. De plus, il est impossible pour un courtier (ou tout autre utilisateur) de modifier un document qui est déjà dans le système.

7. TRANSFERT DE DOSSIERS

NOTE EXPLICATIVE :
Le transfert de dossiers consiste à gérer l'échange des dossiers de courtage immobilier lors des mouvements des courtiers immobiliers (courtier qui change d'agence, cessation d'emploi du courtier, fermeture de l'agence, etc.).

Le concepteur doit donner les détails d'un transfert des dossiers d'une agence (ou courtier à son compte) qui utilise le système décrit ici, **selon trois scénarios** :

- Vers une agence qui utilise le même système.
- Vers un autre système GED.
- Vers le papier (aucun système GED).

7.1. Définition de l'outil de transfert de dossiers

Le concepteur doit décrire le processus de transfert de dossier.

7.2. Gestion des accès à l'outil de transfert de dossiers

Le concepteur doit définir les mécanismes de sécurité d'accès à l'outil de transfert de dossier.

Ce critère est en lien avec la section *3. Sécurité d'accès*, plus particulièrement avec les critères *3.1. Attribution des accès* et *3.2. Groupes d'utilisateurs*.

Exemple :

- ✓ Seuls les utilisateurs du groupe « Administrateur Agence » peuvent accéder aux fonctionnalités de transfert de la solution.

7.3. Mécanisme de transfert

Le concepteur doit indiquer les mécanismes de transfert selon le cas où le destinataire utilise le même système, utilise un autre système de GED ou n'utilise aucun système.

7.4. Sécurité de l'information

Le concepteur indique les méthodes de respect de la confidentialité de l'information lors du transfert de dossiers.

Exemple :

- ✓ Les transferts de dossiers d'un système X vers un autre système X sont effectués par transfert FTP sécurisé (SFTP) qui encrypte les données envoyées et donc garantit la confidentialité des informations transmises.

7.5. Historique

Le concepteur doit décrire les mécanismes de journalisation des transferts de dossiers et :

- ✓ lister toutes les actions de transfert et les groupes d'utilisateurs les effectuant qui déclenchent une entrée dans le journal des transactions d'échange.

- ✓ fournir une copie du journal des transactions de transfert ou de l'accusé de réception de la transaction de transfert.

Exemple :

- ✓ Cet historique peut être généré automatiquement par le système si celui-ci permet le transfert automatisé des dossiers d'un courtier ou d'une agence. L'historique doit inclure la date et l'heure du transfert, le demandeur, les fichiers impactés, le destinataire et l'accusé de réception.
- ✓ Il peut aussi être fait par écrit, sous forme d'accusé de réception signé entre le concepteur de système GED et le courtier ou l'agence. Cet accusé de réception doit inclure la date et l'heure du transfert, le demandeur, les fichiers impactés ainsi que le destinataire.

7.6. Envoi d'une notification à l'OACIQ

Le concepteur ou l'agence doivent informer l'OACIQ lorsqu'une agence utilisant le système GED cesse ses opérations, en indiquant la date de l'envoi des dossiers, le demandeur, les fichiers impactés et le destinataire.

7.7. Conservation de l'information

L'information doit avoir un domaine de résidence sécurisé en tout temps. Dans le cas où l'agence cesse ses activités et qu'aucune agence destinataire n'est assignée, l'agence ou le courtier à son compte doit informer l'OACIQ du lieu d'entreposage des documents pour les prochaines 6 années.

8. RECHERCHE DE DOSSIERS ET DE DOCUMENTS

NOTE EXPLICATIVE :
Les critères de recherche d'une application sont la représentation du concepteur du système des besoins des utilisateurs. Dans ce cas-ci, l'OACIQ constitue un groupe d'utilisateurs et de ce fait, le concepteur doit tenir compte des besoins de recherche des groupes d'inspection et du syndic de l'OACIQ. Ces méthodes de consultations doivent être protégées et réservées aux fins d'inspection et d'enquête de l'OACIQ afin de préserver la confidentialité de l'information.

8.1. Méthodes de recherche de l'OACIQ

Le concepteur doit décrire les mécanismes de recherche des dossiers et des documents réservés à l'Organisme. Si possible, il doit fournir une copie d'écran pour illustrer la fonctionnalité de recherche réservée à l'OACIQ.

8.2. Sécurité des outils de recherche de l'OACIQ :

Le concepteur doit démontrer que les outils de recherche réservés à l'OACIQ sont sécurisés et que seules les autorités reconnues de l'OACIQ ont accès à cette fonctionnalité.

Ce critère est en lien avec la section *3. Sécurité d'accès*, plus particulièrement avec les critères *3.1. Attribution des accès* et *3.2. Groupes d'utilisateurs*.

8.3. Méthode de recherche

Le concepteur doit démontrer que les mécanismes de recherche réservés aux utilisateurs permettent de ne retrouver que les documents auxquels l'utilisateur est autorisé.

Ce critère est en lien avec la section *3. Sécurité d'accès*, plus particulièrement avec les critères *3.1. Attribution des accès* et *3.2. Groupes d'utilisateurs*.

RECOMMANDATIONS FAITES AUX UTILISATEURS ET PROCÉDURES D'UTILISATIONS

Un système conçu en respectant parfaitement les règles de confidentialité, d'intégrité et de conservation de l'information peut être utilisé de façon inadéquate, ce qui entraînerait une faille dans le respect des exigences déontologiques et professionnelles établies par la *Loi sur le courtage immobilier* (L.R.Q., c. C-73.2) et ses différents règlements d'application. C'est pourquoi il est important que les concepteurs d'un système GED fournissent avec leur solution un guide d'utilisation et de recommandations afin que tous les utilisateurs soient bien informés des moyens à prendre pour s'assurer que ces exigences sont respectées et que l'intégrité, la confidentialité et la conservation de l'information ne sont pas mises en péril.

Pour compléter son accréditation, le concepteur doit donc fournir à l'OACIQ la documentation pertinente qui est donnée aux utilisateurs de leur système. Ces documents doivent donner toute l'information nécessaire à tous les groupes d'utilisateurs (gestionnaires d'agences, courtiers, personnel de bureau, etc.) pour que le système soit utilisé de façon à ne pas contrevenir aux exigences déontologiques et professionnelles établies par la *Loi sur le courtage immobilier* (L.R.Q., c. C-73.2) et ses différents règlements d'application.

Les recommandations doivent porter sur, entre autres, les points suivants : l'attribution des accès au système; le retrait des accès; la gestion des accès donnés à des tiers externes (clients, etc.); la gestion des accès au système en cas de système en réseau ou fonctionnant via l'Internet; la procédure à suivre pour la numérisation des documents; la conservation de l'intégrité des documents; etc.