

Vous recevez la présente lettre en votre qualité de représentant autorisé de la société en chef pour votre société pour la Base de données nationale d'inscription (BDNI).

Comme vous le savez, la BDNI contient de l'information sensible, dont la sécurité revêt une importance capitale. Les Autorités canadiennes en valeurs mobilières (ACVM) examinent régulièrement la base de données pour vérifier que les mesures de protection et de contrôle nécessaires ont été mises en place pour protéger ces données. Elles ont, en outre, recours à des services de sécurité reconnus pour surveiller et protéger la BDNI et les données qu'elle contient contre les activités malveillantes.

Malgré les mesures de protection mises en place au niveau du système, toute société qui ne gère pas adéquatement l'accès de ses utilisateurs à la BDNI s'expose à la modification, à la destruction ou à la communication non autorisée de ses données sensibles qui y sont contenues.

La Liste de vérification sur les pratiques exemplaires de gestion des comptes des représentants autorisés de la société (RAS) ci-jointe établie par les ACVM est inspirée des pratiques exemplaires en technologie de l'information prévues par la norme ISO 27002. Bien que les sociétés soient censées avoir déjà instauré leurs propres politiques et procédures de sécurité, les ACVM leur recommandent d'évaluer les processus et contrôles internes existants à la lumière de ces pratiques exemplaires.

Pour de plus amples renseignements, consulter la foire aux questions ci-dessous ou communiquer avec votre autorité principale ou votre organisme d'autoréglementation (OAR), dont vous trouverez les coordonnées sur le site Web d'information de la BDNI au www.nrd-info.ca.

Foire aux questions (FAQ)

Quels sont les risques? Pourquoi la gestion des droits d'accès est-elle si importante?

Comme la BDNI renferme de l'information sensible, toute gestion inappropriée des droits d'accès peut entraîner la modification, la destruction ou la communication non autorisée de cette information.

Qui peut accéder à la BDNI?

Outre les autorités en valeurs mobilières, les représentants autorisés d'une société (RAS) et les personnes physiques inscrites peuvent accéder au site Web de la BDNI et l'utiliser.

Qui peut voir l'information sur l'inscription d'une société ou d'une personne physique dans la BDNI?

Seules les autorités en valeurs mobilières ainsi que les RAS d'une société peuvent accéder à la BDNI et voir l'information sur l'inscription. Les RAS ont uniquement accès à l'information sur l'inscription de leur(s) société(s) et des personnes physiques dont l'inscription est active. Ces dernières peuvent voir leurs formulaires d'inscription initiaux si elles obtiennent l'autorisation de remplir ces formulaires aux fins de dépôt par le RAS.

Quelles sont les pratiques exemplaires recommandées?

Nous recommandons à chaque société de vérifier l'identité de tout utilisateur dont elle configure l'accès, de passer régulièrement en revue les autorisations d'accès dans la Liste des RAS et de révoquer l'accès dès qu'il n'est plus requis.

L'accès utilisateur d'un RAS peut-il être partagé au sein d'une société?

Le partage de l'accès utilisateur n'est pas autorisé. Les ACVM sont déterminés à accroître la sécurité de leurs systèmes de TI, y compris l'accès des utilisateurs.

Le représentant autorisé de la société en chef (le « RAS en chef ») peut configurer l'accès d'autres utilisateurs à la BDNI pour le compte de la société. Les autres RAS peuvent être l'une des personnes suivantes :

- un représentant autorisé de la société (un « RAS »);
- un représentant autorisé de la société administrateur (un « RAS administrateur »).

Une société ne peut avoir qu'un seul RAS en chef, mais peut désigner un nombre illimité de RAS et de RAS administrateurs. Comme tous les RAS peuvent accéder à l'information contenue dans la BDNI, déposer des documents et autoriser des paiements de droits à l'aide de fonds prélevés dans le compte bancaire de la société, il est nécessaire de mettre en place certains contrôles afin de limiter ou de surveiller les activités des utilisateurs. Voici quelques pratiques exemplaires qu'il est possible de mettre en œuvre pour gérer les activités de vos RAS.

Configuration de l'accès des utilisateurs

- Examiner la demande d'accès et prévoir l'approbation par un signataire autorisé.
- Vérifier si la demande d'accès est fondée sur un motif professionnel légitime.

Vérification de l'accès des utilisateurs

- Évaluer trimestriellement la Liste des RAS pour vérifier que seules les personnes ayant besoin d'accéder à la BDNI y ont accès.
- Examiner le compte et le rôle des utilisateurs en cas de modification de l'emploi (comme une cessation d'emploi ou un changement de fonctions).
- Tenir les renseignements sur l'utilisateur à jour (notamment ses courriel et numéro de téléphone).

Révocation de l'accès des utilisateurs

- Révoquer les comptes des utilisateurs qui ne sont plus nécessaires ou pourraient ne plus l'être.
- Révoquer les comptes des utilisateurs immédiatement après un changement de fonctions si l'accès à la BDNI n'est plus requis, ou en cas de cessation d'emploi.

Directives générales sur l'accès des utilisateurs

- Ne pas autoriser le partage de comptes entre utilisateurs.
- Ne jamais partager de mots de passe ni les stocker dans un fichier texte brut.
- N'accorder aux utilisateurs que les privilèges nécessaires à l'exécution de leurs fonctions.
- Ne fournir qu'un seul compte par utilisateur.