Ce guide, à l'usage des consultants qui accomplissent un mandat à la Société, se veut un rappel des obligations en matière **d'éthique, de sécurité de l'information et de protection des renseignements personnels**. Il est important de noter que les obligations présentées dans ce guide ne se substituent pas aux obligations légales ou contractuelles auxquelles sont soumis les consultants.

1 L'ÉTHIQUE

L'éthique est une façon de diriger nos comportements en faisant appel à notre jugement et à notre sens des responsabilités. Elle met l'accent sur les valeurs pour donner un sens à nos décisions et à nos actions. Ainsi, les valeurs apportent un éclairage dans la réflexion préalable à la prise de décision. L'enjeu premier de l'éthique pour une organisation de services publics est de maintenir et de renforcer collectivement la confiance que les citoyens ont envers elle.

Ainsi, le consultant qui travaille à la Société est incité à appuyer ses actions et ses décisions sur les valeurs de l'organisation, soit l'engagement, la rigueur, la cohérence et le respect.

Chacun témoigne de son engagement en adhérant à la vision, à la mission ainsi qu'aux valeurs de la Société et en s'en inspirant quotidiennement.

Manifester son engagement, c'est :

- faire preuve de leadership et influencer le milieu de travail par son comportement exemplaire, son sens critique et le dialogue;
- établir des relations interpersonnelles constructives visant le maintien d'un bon climat de travail;
- mettre en commun les efforts et prendre en compte les compétences particulières ainsi que les préoccupations des autres dans la réalisation de la mission de l'organisation.

L'engagement suppose une motivation du consultant à mettre ses idées et ses habiletés au service de la mission de l'organisation.

Chacun agit avec rigueur, c'est-à-dire avec professionnalisme, intégrité et équité.

Agir avec professionnalisme, c'est :

- s'assurer de respecter les délais prévus avec tout le soin et toute l'attention nécessaires à un travail de qualité;
- chercher à tenir à jour et à améliorer ses connaissances;
- mettre à profit son habileté et son expérience pour atteindre les résultats visés.

Agir avec intégrité, c'est :

- travailler avec honnêteté;
- utiliser de façon judicieuse l'information ou le matériel disponible pour l'exécution de son contrat, et non à des fins personnelles ou au profit d'un tiers;
- préserver son objectivité, son impartialité et sa crédibilité :
    - en s'abstenant d'accorder, de solliciter ou d'accepter toute faveur ou tout avantage indu pour soi-même ou pour une autre personne (par exemple, s'abstenir de communiquer avec un membre du comité de sélection d'adjudication de contrats afin d'influencer le processus d'adjudication ou de tenter d'obtenir plus de détails quant au résultat d'adjudication);
    - en évitant toute situation de conflit d'intérêts, réel ou apparent, et si une telle situation se présente, en informer immédiatement la Société.

Agir avec équité, c'est :

- apprécier avec justesse ce qui est dû à chacun en faisant preuve :
    - d'égalité de traitement (égalité devant la loi);
    - d'impartialité (intervenir sans préjugé ni discrimination);
    - de jugement (reconnaître les particularités et les différences de certaines personnes pour assurer un juste traitement de leur dossier).

Chacun agit en toute cohérence avec la Société.

Agir avec cohérence, c'est :

- favoriser l'esprit d'équipe;
- communiquer efficacement afin de favoriser la coordination des interventions et la production de services de qualité au meilleur coût;
- être responsable, c'est-à-dire :
    - respecter les lois et les normes applicables au travail confié;
    - arrêter ses choix en considérant les conséquences sur les parties impliquées;
    - pouvoir justifier ses décisions et en assumer les conséquences.

Chacun agit avec respect en maintenant une relation de confiance.

Agir avec respect, c'est :

- être poli et courtois dans ses gestes et ses paroles;
- faire preuve de transparence et d'écoute;
- faire preuve de discrétion et de retenue;
- s'abstenir de toute violence ou de tout harcèlement;
- dans ses communications, se présenter en précisant son statut et son mandat, y compris lors des réunions;
- permettre au personnel de la Société de respecter ses obligations de confidentialité et de protection des renseignements personnels;
- permettre aux professionnels de la Société de respecter leur obligation au secret professionnel;
- si un avis juridique est requis, demander au gestionnaire responsable de son contrat de faire une demande à la Direction des affaires juridiques.

2 LA SÉCURITÉ DE L'INFORMATION

La Société a mis en place diverses mesures de sécurité pour s'assurer de la confidentialité, de l'intégrité et de la disponibilité de l'information qu'elle détient. Il est de votre responsabilité de respecter ces mesures tout au long de votre mandat.

UTILISATION DE VOTRE CODE D'UTILISATEUR

Ce code sert à établir votre identité et à vous permettre d'accéder aux données dont vous avez besoin pour effectuer votre mandat. Il vous est attribué lors de votre entrée en fonction à la Société et est à votre usage exclusif. Vous êtes responsable des accès effectués sous votre code d'utilisateur.

Il est essentiel de verrouiller votre session lorsque vous vous absentez de votre poste de travail.

UTILISATION DE VOTRE MOT DE PASSE

Le mot de passe sert à valider votre identité. Il est important de le garder secret, sans quoi une personne qui le connaît pourrait usurper votre identité. Elle pourrait ainsi consulter, modifier ou même détruire des données et effectuer des opérations qui vous seraient imputées.

Si vous croyez que quelqu'un connaît votre mot de passe, vous devez immédiatement le changer.

UTILISATION D'UNE CLÉ USB

Si vous devez utiliser une clé USB pour le transport d'informations, vous êtes tenu d'utiliser une clé USB sécuritaire, qui :

- est pourvue d'un mécanisme de chiffrement;
- permet le chiffrement automatique de toutes données copiées sur la clé;
- est dotée d'un algorithme de chiffrement robuste (AES 256 bits au minimum);
- qui répond en conformité à la norme FIPS 140-2 « Level 2 » au minimum.

À titre d'exemple, la clé USB « Kingston DataTraveler Vault ou 4000G » répond aux exigences de sécurité de la Société.

L'information qui n'est plus utile doit être supprimée de la clé USB dès que possible.

En cas de perte de la clé USB :

- informez immédiatement le gestionnaire de la Société;
- déterminez la nature exacte des documents sur la clé;
- si des documents personnels ou confidentiels s'y trouvaient, la Procédure pour encadrer les bris de confidentialité doit être effectuée.

UTILISATION DU COURRIEL

Seule l'adresse de courriel se terminant par « @saaq.gouv.qc.ca » doit être utilisée lors de communications effectuées au nom de la Société. Il est interdit dans ce contexte d'inclure une référence à votre firme dans la signature du courriel.

Il est interdit de transmettre à l'extérieur de la Société – par courriel, par collecticiel, par Internet ou par un autre moyen – tout renseignement de nature confidentielle qui n'a pas fait l'objet d'un chiffrement.

Vous ne devez jamais rediriger un « courriel SAAQ » sur un réseau non protégé (par exemple, sur un téléphone intelligent, à votre entreprise, à un autre ministère ou à un autre organisme, ou à votre domicile). De même, vous ne devez jamais inciter un employé de la Société à vous transmettre des documents confidentiels sur des réseaux externes.

Toute information stockée ou consignée sur l'équipement électronique de la Société à l'aide d'un courriel, d'un collecticiel, d'Internet, ou par tout autre moyen est réputée constituer une information à laquelle la Société a accès. Ainsi, la Société peut récupérer le contenu des boîtes de courriel si elle le juge opportun.

Enfin, au terme de votre mandat, vous devez effacer de votre boîte de courriel les renseignements personnels et les autres informations qui vous appartiennent. L'utilisation du courriel est un privilège qui peut vous être enlevé en tout temps pour tout motif jugé raisonnable.

UTILISATION D'INTERNET

L'utilisation d'Internet est permise uniquement pour l'accomplissement de votre mandat à la Société.

La Société tient un registre quotidien des sites Internet visités par chaque utilisateur. Rappelez-vous que certains sites recueillent l'adresse de leurs visiteurs et publient parfois des statistiques à ce sujet. La Politique d'utilisation du courriel et des services d'Internet de la Société précise que : « les outils électroniques rendent possible l'identification de la Société par un interlocuteur externe, et il faut en tenir compte lors de leur utilisation ».

Pour plus d'information, consultez la Politique d'utilisation du courriel et des services d'Internet de la Société.

SIGNALEMENT DES INCIDENTS

Vous devez rapporter rapidement tout problème de sécurité informatique (code malveillant, virus informatique, etc.) au Centre de services en technologies de l'information de la Société (418 528-3210).

CONFIDENTIALITÉ DE L'INFORMATION

L'information communiquée par la Société est confidentielle, de même que celle que vous devez produire dans le cadre de votre mandat. À titre d'exemple, il peut s'agir de documentation ou d'information concernant des projets de développement, des plans d'action, des façons de faire actuelles ou envisagées, des mécanismes de sécurité, des contrôles ou des problèmes à corriger. Sauf si votre contrat de service prévoit le contraire ou si vous obtenez l'autorisation d'un représentant de la Société, cette information appartient à la Société et doit demeurer dans ses bureaux.

- Vous ne pouvez pas utiliser cette information à d'autres fins que la réalisation de votre mandat.
- Il vous est interdit de faire des copies des documents, que ce soit pour un usage personnel ou professionnel, ou pour une référence future.
- Vous ne pouvez pas communiquer l'information à d'autres personnes, à moins que cela ne soit requis pour l'exécution du mandat.

CONFIDENTIALITÉ DES DONNÉES INFORMATIQUES

La Société détient de nombreux renseignements sur ses usagers, son personnel et ses fournisseurs. Tous les renseignements se rapportant à des personnes physiques sont des renseignements personnels et confidentiels. Les renseignements se rapportant à des personnes morales et les autres données inscrites dans les systèmes informatiques de la Société sont aussi des renseignements confidentiels, même s'ils ne sont pas des renseignements personnels.

- La Société effectue des vérifications quotidiennes des consultations faites dans ses systèmes d'information.
- Il vous est strictement interdit de consulter et d'utiliser ces renseignements à d'autres fins que la réalisation de votre mandat.
- Avant de pouvoir accéder à des renseignements confidentiels sur les clientèles, le personnel ou les fournisseurs de la Société, vous devez signer un formulaire d'engagement à la confidentialité.
- Vous devez utiliser des données fictives pour les essais de système et les autres tests.

3 PROTECTION DES RENSEIGNEMENTS PERSONNELS

Afin d'assurer la confidentialité des renseignements personnels, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* énonce des règles précises. La Société les met en œuvre à l'aide des politiques et des procédures de son cadre de gestion accessibles dans l'intranet.

L'ACCÈS AUX RENSEIGNEMENTS PERSONNELS

Toute personne physique a droit à la confidentialité des renseignements qui la concernent. Elle (ou son représentant autorisé) a le droit d'y accéder, d'en demander copie, ou de les faire rectifier.

Remarque : Vous n'êtes pas autorisé à traiter les demandes d'accès ou de rectification. Elles doivent être adressées à la Société le plus rapidement possible.

LA COLLECTE DE RENSEIGNEMENTS PERSONNELS

Lorsque votre contrat de service vous autorise à recueillir des renseignements personnels pour le compte de la Société, vous ne pouvez le faire que si ces renseignements sont nécessaires au traitement du dossier de la personne concernée ou à l'exécution de votre contrat.

La personne à qui l'on demande un renseignement personnel doit être informée :

- du nom et de l'adresse de la Société;
- des fins pour lesquelles ce renseignement est recueilli;
- des catégories de personnes qui auront accès à ce renseignement;
- du caractère obligatoire ou facultatif de la demande;
- des conséquences en cas de refus de répondre à la demande;
- des droits d'accès et de rectification.

Un avis à cette fin doit être inclus dans tout formulaire de collecte de renseignements personnels ou joint à celui-ci. Son contenu doit être approuvé par la Société.

L'UTILISATION DES RENSEIGNEMENTS PERSONNELS AU SEIN DE LA SOCIÉTÉ

L'utilisation de renseignements personnels sans le consentement de la personne concernée est strictement encadrée.

Seules les personnes préalablement autorisées par la Société peuvent accéder aux renseignements personnels nécessaires à l'exercice de leurs fonctions selon les accès qui leur sont attribués.

Vous ne devez ni prendre connaissance ni utiliser les renseignements personnels détenus par la Société, sauf lorsqu'ils sont nécessaires à l'exercice des fonctions et des tâches qui vous sont confiées.

La curiosité ou l'intérêt personnel ne justifient pas la consultation ou l'utilisation de renseignements personnels.

Les renseignements personnels que vous utilisez pour rendre une décision au sujet d'une personne physique doivent être versés au dossier de cette personne, quel que soit le support sur lequel ces renseignements sont regroupés.

Les renseignements personnels détenus par la Société doivent être à jour, exacts et complets pour servir aux fins pour lesquelles ils ont été recueillis.

LA COMMUNICATION DE RENSEIGNEMENTS PERSONNELS À UN TIERS

Lorsque votre contrat de service exige que vous communiquiez des renseignements personnels à des tiers, vous devez d'abord obtenir l'autorisation de la personne concernée. Cette autorisation doit être claire, donnée à des fins précises, et pour une durée déterminée.

En l'absence du consentement de la personne concernée, la communication de renseignements personnels à des tiers doit être préalablement approuvée par la Société et respecter les exigences administratives et de sécurité fixées par la Société.

LA CONSERVATION ET LA DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

Les exigences de la Société relatives à la conservation et à la destruction des documents sont indiquées dans votre contrat de service. Nous tenons toutefois à vous rappeler que vous ne pouvez pas utiliser à des fins personnelles des documents qui contiennent des renseignements personnels ou des informations

confidentielles destinés à être jetés ou détruits. Le mode de destruction des documents contenant des renseignements personnels doit assurer la protection de la confidentialité.

Pour obtenir plus d'information, consultez la fiche d'information qui est jointe à votre contrat de service.

L'UTILISATION DU TÉLÉCOPIEUR

Lorsque vous avez à transmettre par télécopieur des documents contenant des renseignements personnels, vous devez respecter les règles contenues dans la procédure pour l'envoi de documents confidentiels par télécopieur. Cette procédure prévoit notamment qu'avant d'entreprendre une communication par télécopieur, il est nécessaire de s'assurer que le destinataire est autorisé à obtenir les renseignements devant lui être communiqués.

CONSÉQUENCES DU NON-RESPECT DE CES RÈGLES

Le non-respect de ces règles constitue un manquement aux obligations de confidentialité du consultant.

Un bris de confidentialité résultant du non-respect de ces règles aurait des conséquences néfastes pour la Société. Il en aurait aussi pour le consultant, qui s'exposerait à des poursuites civiles, voire pénales, dans le cas d'un bris intentionnel, en plus d'autres conséquences prévues au contrat.

SÉCURITÉ DES PERSONNES ET DES BIENS

La Société a élaboré et mis en place des règles, des mesures de sécurité et des plans des mesures d'urgence pour assurer la sécurité physique des personnes et des biens dans ses établissements. Ces éléments contribuent également à la sécurité de l'information et à la continuité des services offerts. Il est de la responsabilité des fournisseurs ainsi que de leur personnel d'en prendre connaissance en début de mandat, de les connaître et de les respecter tout au long de leur contrat ou de leur mandat avec la Société.

En ce qui a trait aux règles et aux mesures de sécurité pour le siège social, veuillez consulter l'annexe du présent guide pour un résumé. Pour ceux travaillant à l'extérieur du siège social, veuillez vous référer auprès du gestionnaire de l'établissement dans le réseau provincial, auprès de la Direction des ressources matérielles et immobilières au siège social ou à la tour de la Bourse.

Concernant le Plan des mesures d'urgence, chacune des personnes doit connaître les procédures propres à chaque situation d'urgence et l'emplacement des sorties de secours pour l'établissement occupé. Pour obtenir les informations pertinentes, veuillez vous référer à l'intranet de la Société à la section « Urgences »; auprès du gestionnaire de l'établissement dans le réseau provincial, auprès de la Direction des ressources matérielles et immobilières au siège social ou à la tour de la Bourse.

ANNEXE

RÈGLES D'ACCÈS AU SIÈGE SOCIAL

Résumé

Définitions

Employé externe : Cadre, consultant ou travailleur d'un fournisseur externe.

Employé interne : Employé permanent, occasionnel, étudiant ou stagiaire, inscrit au répertoire du personnel.

Employé inscrit d'un fournisseur autorisé : Personne inscrite par le chargé de projet de la SAAQ comme étant employée d'un fournisseur autorisé. Elle n'est pas considérée comme un employé externe.

Fournisseur autorisé : Organisation liée par contrat avec la Société.

Répertoire du personnel : Disponible par la page d'accueil de l'intranet.

Visiteur : Toute personne autre qu'un membre du personnel de la Société ou du personnel d'un fournisseur autorisé.

Généralités

Toute personne qui accède au périmètre sécurisé du siège social doit être conformément enregistrée au système de contrôle d'accès de la sécurité. Une personne non enregistrée, présente dans la zone sécurisée, en sera immédiatement expulsée.

Toute entrée ou sortie du périmètre sécurisé ainsi que tout accès aux locaux sécurisés des personnes doivent être enregistrés au système de contrôle d'accès. Cet enregistrement se fait par la lecture de la carte d'accès de chacune des personnes.

Détenteurs autorisés ou non d'une carte d'accès; les membres du personnel interne et externe ainsi que les fournisseurs et leurs employés doivent respecter les règles d'accès au siège social.

1. Règles d'utilisation de la carte d'accès

1.1. Le détenteur autorisé est responsable de sa carte d'accès. À cet effet, il doit :

a. Conserver de façon sécuritaire sa carte d'accès;

b. Signaler rapidement toute perte, tout vol, toute utilisation frauduleuse ou tout bris de sa carte d'accès;

c. Ne prêter sa carte d'accès, pour aucune raison;

d. Signaler tout problème concernant les droits d'accès permis par sa carte d'accès.

1.2. Pour tout accès requérant l'utilisation de sa carte d'accès, le détenteur autorisé doit s'assurer qu'aucune autre personne ne profite de l'ouverture pour s'introduire frauduleusement. S'il constate un tel acte, réussi ou non, le détenteur autorisé doit signaler l'incident sans délai à un agent de sécurité, directement ou par le biais de la ligne d'urgence 4911 ou 418 528-4911.

1.3. Le personnel interne et externe ainsi que les fournisseurs et leurs employés, non détenteurs autorisés d'une carte d'accès au siège social, ne peuvent emprunter ou utiliser l'une d'elles, pour aucune raison.

2. Procédure d'accès du personnel sans carte d'accès

Voir la documentation complète dans l'intranet.

3. Procédure d'accès d'un visiteur

Voir la documentation complète dans l'intranet.

4. Procédure d'accès à un fournisseur

Voir la documentation complète dans l'intranet.

5. Personne avec besoin d'accès spéciaux (p. ex. : personne handicapée)

S'adresser à un agent de sécurité pour obtenir les autorisations nécessaires à sa condition.

6. Accès à la garderie

Se présenter au poste de garde de l'entrée principale (porte Ouest).

Dès que vous aurez accès à l'intranet, vous devrez prendre connaissance de la documentation complète.