GRAND THÉÂTRE QUÉBEC

POLITIQUE SUR LA SÉCURITÉ INFORMATIQUE ET SUR L'UTILISATION DES RESSOURCES INFORMATIQUES DE LA SOCIÉTÉ DU GRAND THÉÂTRE DE QUÉBEC

Juin 2008

Adoptée : Rés. CA 2008-303
Mise à jour : Rés. CA 2012-332

1. DISPOSITIONS GÉNÉRALES

La présente politique décrit les lignes directives adoptées par la Société du Grand Théâtre de Québec (ci-après « la Société ») en matière d'informatique. Ce document résume les points les plus importants devant être compris et mis en pratique par tous les employés de la Société. De plus, il précise les attentes minimales auxquelles tout membre du personnel doit répondre lors de l'utilisation d'un accès au courriel, aux services Internet et de l'utilisation de l'équipement informatique mis à sa disposition.

L'objectif poursuivi par la politique est d'établir des pratiques visant la protection des renseignements personnels et celle de l'information concernant les affaires de la Société ainsi que de ses environnements informatiques.

Elle définit les pratiques à implanter en termes de mesures de contrôle dans les systèmes et réseaux où le traitement des affaires de la Société est effectué, et où la disponibilité, l'intégrité et la confidentialité font partie des attentes de ses utilisateurs.

La conformité à cette politique est obligatoire et sujette à vérification.

Les transgressions à la présente politique seront traitées selon les règles applicables en matière de discipline, s'il y a lieu.

Toute dérogation à la présente politique doit être justifiée et documentée.

2. IDENTIFICATION ET AUTHENTIFICATION DES UTILISATEURS

L'équipement informatique de la Société ainsi que les logiciels dont elle détient une licence d'utilisation sont réservés exclusivement à l'usage des employés de la Société, ainsi qu'à tout intervenant externe, consultant, contractuel ou fournisseur, dûment autorisé par la Société. Chaque utilisateur autorisé doit s'identifier au système informatique et doit être en mesure de prouver cette identité. Cette identification s'effectue par le biais d'un code d'accès et l'authentification à l'aide d'un mot de passe.

- **Les codes d'accès aux systèmes**

Un code d'accès à un système informatique est réservé à l'usage exclusif d'une seule et unique personne. Ce code d'accès doit être validé par le système informatique lors du début d'une session de travail, quelle que soit la plate-forme technologique utilisée.

- **Le mot de passe**

Le mot de passe doit faire l'objet d'une vérification au début de chaque session de travail, et sert à authentifier l'utilisateur détenteur du code d'accès. Ce mot de passe est strictement confidentiel. Il doit être mémorisé et ne doit pas être écrit. L'utilisateur doit prendre des mesures raisonnables pour préserver la confidentialité de son mot de passe. Il veillera notamment à ne pas le divulguer à d'autres personnes. Le mot de passe est personnel, c'est la signature de l'utilisateur. Il engage sa responsabilité lorsqu'il accède aux systèmes d'information.

- Qualité et robustesse du mot de passe

Le mot de passe constitue la première ligne de défense dans l'ensemble des mesures mises en place pour protéger les ressources informationnelles de la Société. Il doit donc correspondre à certains critères de sécurité, de qualité et de robustesse.

Il doit :

1. avoir une longueur minimale de 8 caractères;
2. être de format alphanumérique;
3. être différent du dernier mot de passe utilisé;
4. être différent du nom, du prénom et du code d'accès de l'utilisateur;
5. utiliser des majuscules et des minuscules.

Il ne doit pas :

1. contenir plus de deux (2) caractères répétitifs;
2. correspondre à des chaînes de caractères consécutifs sur le clavier;
3. être facile à deviner;
4. être un mot commun que l'on peut retrouver dans le dictionnaire;
5. correspondre à une terminologie typique de la Société.

- Changement du mot de passe

Le mot de passe doit être changé tous les quatre-vingt-dix (90) jours et ce changement doit être imposé par le système informatique, quelle que soit la plate-forme technologique.

Lorsqu'un utilisateur oublie son mot de passe, il peut le faire réinitialiser par le directeur de l'administration. Dans un tel cas, le mot de passe émis par le directeur de l'administration ne doit être valide qu'une seule fois, c'est-à-dire qu'il doit expirer dès sa première utilisation. L'utilisateur doit donc le changer en conformité avec les critères précédemment énoncés.

De plus, le compte de l'usager sera désactivé après trois (3) tentatives infructueuses de connexion au réseau.

- Mot de passe administrateur

Le compte « Administrateur » représente le compte utilisateur le plus à risque dans un système d'exploitation dû à ses droits d'accès illimités. Il est donc primordial de contrôler son utilisation ainsi que de renforcer la sécurité de son mot de passe. Le mot de passe du compte « Administrateur » doit donc respecter les critères suivants :

A) dans le cas où la Société a son propre département d'informatique :

– il doit être modifié tous les quatre-vingt-dix (90) jours par le directeur de l'administration;

- il doit être conservé dans une enveloppe scellée à un endroit sécuritaire. Cette enveloppe devra être utilisée seulement lors d'une urgence où le directeur de l'administration n'est pas présent. Lorsque l'enveloppe est utilisée, le mot de passe doit être modifié aussitôt que possible et une nouvelle enveloppe devra être créée;

- seulement le directeur de l'administration doit connaître le mot de passe du compte « Administrateur »;

- le mot de passe doit avoir une longueur minimale de 8 caractères et être une combinaison de lettres, de chiffres et d'un caractère spécial (!,+,$,-,%,?,&,*,#,|,...). De plus, tous les mots de passe des comptes ayant des droits d'administrateur doivent respecter ces critères;

- le compte « Administrateur » doit être utilisé seulement par le directeur de l'administration et en aucun cas son mot de passe ne doit être divulgué à un employé (à moins d'une urgence où l'enveloppe devra être utilisée).

B) dans le cas où la Société utilise les services d'une firme externe :

- il doit être modifié tous les quatre-vingt-dix (90) jours par la firme externe;

- seul le directeur de l'administration et le personnel de la firme externe doit connaître le mot de passe du compte « Administrateur »;

- le mot de passe doit avoir une longueur minimale de 8 caractères et être une combinaison de lettres, de chiffres et d'un caractère spécial (!,+,$,-,%,?,&,*,#,|,...). De plus, tous les mots de passe des comptes ayant des droits d'administrateur doivent respecter ces critères;

- le compte « Administrateur » doit être utilisé seulement par le directeur de l'administration ou un membre de la firme externe et en aucun cas son mot de passe ne doit être divulgué à un employé.

- **Utilisation d'un code d'accès**

Le détenteur d'un code d'accès aux systèmes informatiques de la Société est responsable et imputable des actes posés avec son code d'accès. Ce code doit donc être géré et utilisé en conformité avec les règles précédemment énoncées.

Lors d'une absence temporaire pendant laquelle le code d'accès d'un détenteur doit être utilisé par quelqu'un d'autre pour assurer la continuité d'une ou plusieurs activités, le détenteur doit aviser par écrit son supérieur immédiat de la situation, en spécifiant par qui, pour combien de temps et pour quelle raison son code d'accès doit être utilisé par quelqu'un d'autre. Une copie conforme de cet avis doit être remise au directeur de l'administration. À son retour au travail, le détenteur doit modifier son mot de passe immédiatement.

- **Utilisation pour fins de travail seulement**

Les équipements informatiques ainsi que les logiciels fournis par la Société à ses employés, contractuels, consultants et fournisseurs ne doivent être utilisés qu'à des fins de travail. L'utilisation de ces équipements et logiciels peut être vérifiée par la Société en tout temps.

- **Privilèges d'accès**

Lorsqu'un utilisateur quitte la Société, prend un congé prolongé de plus d'un mois, ou n'a plus un besoin de travail valide justifiant des accès aux systèmes informatiques de la Société, son supérieur immédiat doit en aviser le directeur de l'administration. Ce dernier doit disposer d'un processus et/ou de contrôles techniques permettant d'interdire l'accès aux systèmes immédiatement après la réception de l'avis du supérieur immédiat.

Le supérieur d'un employé faisant l'objet d'une mutation doit aviser le(s) détenteur(s) des systèmes d'information auxquels il a accès dans le cadre de son travail, ainsi que le directeur de l'administration de ce mouvement de personnel. On doit alors s'assurer que les privilèges d'accès qui ne sont plus nécessaires soient effectivement retirés au code d'accès de l'utilisateur concerné.

Lors d'un congédiement, le supérieur immédiat de la personne concernée doit aviser le directeur de l'administration de l'événement avant le fait. Ce dernier doit voir au retrait des privilèges d'accès de la personne concernée avant qu'elle ne soit avisée de son congédiement. Le tout doit se dérouler dans la plus stricte confidentialité.

Lors de l'arrivée d'un nouvel employé, le directeur de l'administration doit l'informer de l'existence des normes de sécurité informatique, et ensuite lui faire signer le formulaire reproduit à l'Annexe 1.

3. PROTECTION DES RESSOURCES INFORMATIONNELLES

- **Programmes anti-virus**

Le directeur de l'administration est responsable de l'acquisition et de la mise en place d'un outil de protection contre les virus informatiques.

- Les programmes anti-virus doivent être configurés de façon à rechercher les nouveaux virus au moins une fois par semaine;

- La mise à niveau du programme de détection de virus doit être effectuée avant la désuétude du logiciel;

- La mise à niveau du fichier de signatures de virus doit être effectuée immédiatement lorsqu'une nouvelle version est disponible;

- Le directeur de l'administration est responsable de l'élaboration et de la mise en place d'un processus de réaction immédiate dans l'éventualité où un poste de travail ou un serveur deviendrait infecté par un virus informatique.

- **Gestion des licences de logiciels**

Seuls les logiciels pour lesquels la Société détient une licence d'utilisation en bonne et due forme peuvent être utilisés dans l'environnement informatique de la Société. Le directeur de l'administration est responsable de l'élaboration et de la mise en place d'un processus visant à s'assurer de la conformité d'utilisation par le biais, par exemple, d'un inventaire automatique et périodique des logiciels se trouvant sur les postes de travail. Le processus doit également prévoir la suppression de tout logiciel pour lequel la Société ne détient pas de licence.

4. RAPPORT DE TRANSGRESSION

Toute transgression ou tentative d'infraction aux règles de sécurité doit faire l'objet d'un suivi. Tous les accès refusés par les mécanismes de contrôle d'accès doivent faire l'objet d'une journalisation.

Tous les débuts et fins de session doivent faire l'objet d'une journalisation. La fonction de journalisation doit être active en tout temps, sans exception (gérée par les utilitaires du serveur).

Le directeur de l'administration est responsable de l'élaboration et de la mise en place d'un processus visant à produire des rapports sur les tentatives de branchement infructueuses. Le processus doit également prévoir un suivi sur ces activités.

Le directeur de l'administration est responsable de l'élaboration et de la mise en place d'un processus permettant de détecter les attaques systématiques (tentatives de branchement infructueuses à répétition). Le processus doit également prévoir une escalade lorsque l'envergure de l'attaque dépasse un certain niveau (compte désactivé après trois (3) tentatives infructueuses).

Le directeur de l'administration est responsable de l'élaboration et de la mise en place d'un processus vérifiable de suivi sur ces transgressions. Le processus doit prévoir que le détenteur de la ressource visée ainsi que le supérieur immédiat de la personne concernée soient avisés de la tentative d'accès.

5. PROTECTION DES POSTES DE TRAVAIL

- **Protection contre les virus**

Tous les postes de travail de la Société de même que les serveurs doivent être équipés d'un mécanisme de protection contre les virus informatiques. La désactivation de ce mécanisme par l'employé utilisateur du poste est interdite. Le mécanisme doit être configuré de manière à effectuer un balayage du disque dur du poste à intervalles réguliers. Sa configuration doit également prévoir le balayage systématique des supports insérés dans les lecteurs.

Le directeur de l'administration est responsable de l'élaboration et de la mise en place d'un processus de réaction lors de la détection d'un virus informatique. Le processus doit prévoir :

- la réaction immédiate (isolation du poste de travail);
- l'identification du virus;
- l'enlèvement du virus;

- le cas échéant, la récupération des données perdues lorsque cela est possible;
- l'investigation sur la façon dont le poste a été infecté;
- l'évaluation des dégâts.

- **Dispositif de mise en veille**

Tous les postes de travail de la Société doivent être équipés d'un mécanisme de mise en veille. Ce mécanisme doit toujours être en fonction. Un mot de passe doit être requis pour la désactivation de ce mécanisme. Le mot de passe doit correspondre aux critères de qualité et de robustesse énoncés à la section 2 (c'est le même mot de passe que pour l'ouverture de session réseau).

- **Installation de logiciels dans les postes de travail**

Seul le personnel autorisé peut procéder à l'installation de logiciels sur les postes de travail. Seuls les logiciels pour lesquels la Société détient une licence d'utilisation en bonne et due forme peuvent être utilisés dans les environnements informatiques de la Société. Les postes de travail sont inclus dans cette description. Le directeur de l'administration est responsable de la vérification de ces derniers et toute transgression fera l'objet d'un rapport à la direction générale.

- **Sauvegarde des fichiers**

L'utilisateur doit être conscient que les documents conservés sur le disque dur de son ordinateur ne sont jamais pris en sauvegarde par le réseau informatique et qu'il existe un risque de perdre ces documents advenant un bris d'équipement. Afin de minimiser les risques de perdre des documents importants, l'utilisateur devrait toujours sauvegarder ses fichiers sur le réseau informatique, dans un répertoire personnel.

Parallèlement à la sauvegarde des fichiers, tout fichier sauvegardé dans un répertoire personnel sur le réseau informatique doit être en lien avec le travail à la Société. Tout fichier, document, texte, photo qui n'est pas un lien avec le travail à la Société ne doit être sauvegardé sur le réseau informatique.

6. UTILISATION DU RÉSEAU INTERNET ET DU COURRIER ÉLECTRONIQUE

- **Utilisation pour fins de travail seulement**

Les employés de la Société qui ont la possibilité d'utiliser le réseau Internet via les facilités mises à leur disposition par la Société ne doivent utiliser cet outil que pour des activités reliées à leur travail pour la Société. L'utilisation de ces outils est sujette à vérification par le directeur de l'administration. Les utilisateurs doivent prendre en compte le fait que le courrier électronique et le réseau Internet ne doivent pas servir notamment à :

- envoyer des chaînes de lettres à des tiers;
- harceler un autre membre du personnel ou toute autre personne;
- recevoir des courriels de serveurs de listes à d'autres fins que professionnelles;
- visionner, télécharger, copier, partager ou expédier des images ou des fichiers de type pornographique ou dont le contenu a un caractère diffamatoire, offensant, sexiste, haineux, violent, menaçant ou raciste;
- utiliser à des fins personnelles les moyens électroniques mis à sa disposition;
- utiliser des messageries instantanées.

- **Gestion de la boîte aux lettres**

L'utilisateur veillera à gérer adéquatement sa boîte aux lettres, en :

- prenant connaissance de son courrier régulièrement et en traitant les messages dans un délai raisonnable;
- transmettant les courriers électroniques contenant des pièces jointes volumineuses hors des heures durant lesquelles le réseau est très utilisé. (Il faut éviter si possible les fichiers de plus de 4 Mo et les plages horaires de 9 h à 11 h et de 13 h 30 à 15 h 30);
- détruisant les courriers électroniques lorsque l'information contenue n'est plus utile.

- **Téléchargement de logiciels**

Le téléchargement de logiciels à partir du réseau Internet dans l'environnement informatique de la Société est réservé au personnel autorisé seulement. Tout logiciel téléchargé doit systématiquement faire l'objet d'un balayage permettant de détecter la présence de virus informatiques avant toute utilisation. Le téléchargement d'un logiciel à partir du réseau Internet doit également faire l'objet d'une justification reliée au travail. Le directeur de l'administration est responsable de désigner le personnel autorisé à effectuer de tels téléchargements.

- **Sites Internet à contenu répréhensible**

Certains sites sur le réseau Internet contiennent des images ou des textes considérés comme répréhensibles au sens des lois (pornographie juvénile, racisme, etc.). Il est strictement interdit d'accéder à ces sites via l'environnement informatique de la Société. Toute infraction à cette règle doit être détectée. Lorsqu'il est déterminé que l'accès ou la tentative d'accès est volontaire, le supérieur immédiat du contrevenant doit être informé, lors d'une première infraction. En cas de répétition, le directeur de l'administration prend les mesures qui s'imposent dans les circonstances. Tout matériel de ce genre doit être détruit aussitôt trouvé. Le stockage sur l'équipement informatique de la Société de matériel offensant est également interdit.

- **Utilisation du coupe-feu**

Le mur coupe-feu (firewall) gère l'accès aux ressources réseau. Il a pour principale tâche de contrôler le trafic entre le réseau Internet et le réseau local de la Société. Le but ultime est de fournir une connexion contrôlée, en bloquant les intrusions en provenance d'Internet et de contrôler le trafic sortant vers Internet (bloquer certains sites, messageries instantanées, etc…). Le directeur de l'administration est responsable de la mise en place et du bon fonctionnement du coupe-feu.

- **Suivi sur les transgressions aux règles**

Toute infraction ou tentative d'infraction aux règles programmées dans le coupe-feu ou dans les filtres doit faire l'objet d'un suivi et, le cas échéant, d'un avis au contrevenant ainsi qu'à son supérieur immédiat.

7. LES POSTES OUVERTS AU PUBLIC

- **Le réseau des postes publics**

Le réseau par lequel seront reliés les postes ouverts au public est isolé physiquement, logiquement et électroniquement de l'environnement informatique corporatif. Il ne doit exister aucun chemin d'accès entre les deux.

- **Journalisation des activités**

Tous les accès au réseau Internet effectués via les postes publics doivent être journalisés. Ce journal ne doit être accessible que lors d'enquête dûment mandatée. En tout autre temps, ce journal demeure inaccessible. Le directeur de l'administration est responsable de l'élaboration et de la mise en place d'un processus vérifiable et démontrable, visant l'isolation de ce journal et sa consultation par des personnes temporairement autorisées, le cas échéant.

8. LE REGISTRE D'AUTORITÉ

Le tableau qui suit constitue la base du registre d'autorité devant être maintenu par la Société. Il identifie les systèmes d'information (actuels ou futurs) ainsi que leurs détenteurs. On devra également y joindre, à titre d'information complémentaire, les différents profils d'accès (selon les postes occupés) à ces systèmes d'information, et finalement, les noms des employés permanents, temporaires, consultants et contractuels reliés à ces profils d'accès.

Système d'information	Détenteur
Site WEB	Service du marketing
Ventilation	Service de l'immeuble
Système comptable	Direction de l'administration
Système de paie	Direction de l'administration
Système poste à l'accueil	Service de l'accueil
Gestion documentaire	Direction de l'administration
Journaux informatiques	Direction de l'administration
Système de billetterie	Service de la billetterie
Système d'accès au stationnement	Service de l'immeuble

9. ENCADREMENT ET CONTRÔLE

Toute information enregistrée ou consignée sur l'équipement électronique de la Société au moyen du courriel ou des services Internet ou par tout autre moyen, est réputée constituer une information à laquelle la Société a accès.

La Société peut appliquer des mesures de gestion appropriées, selon les circonstances, à l'information qui est propre à un employé et que ce dernier a enregistrée sur l'équipement électronique de la Société.

La Société pourra effectuer des vérifications régulières de l'utilisation d'un accès au courriel ou aux services Internet pour des motifs opérationnels et procédera à l'analyse de leurs résultats.

La Société peut décider de soumettre un membre de son personnel à une vérification particulière de l'utilisation d'un accès au courriel, à un collecticiel ou aux services Internet, lorsqu'il existe des raisons de soupçonner que cette utilisation n'est pas conforme à la présente directive.

- **Sanction**

La Société détermine, selon la nature ou la gravité des cas, s'il est opportun d'appliquer une sanction disciplinaire ou de prendre une mesure administrative lorsqu'un membre de son personnel contrevient aux directives de la présente politique.

ANNEXE 1

CONVENTION DE L'UTILISATEUR DU RÉSEAU INFORMATIQUE DE LA SOCIÉTÉ DU GRAND THÉÂTRE DE QUÉBEC INCLUANT L'USAGE DE L'INTERNET ET DU COURRIER ÉLECTRONIQUE

J'ai obtenu copie et pris connaissance de la politique sur la sécurité informatique et sur l'utilisation des ressources informatiques en date du _____. Je reconnais et je comprends que l'usage de l'environnement informatique de la Société du Grand Théâtre de Québec incluant l'usage de l'Internet et du courrier électronique ne doit avoir lieu que dans le cadre des activités de cette dernière.

En tant qu'employé du Grand Théâtre, consultant, contractuel, fournisseur ou toute autre personne travaillant de façon temporaire ou permanente pour la Société, je comprends que la politique sur la sécurité informatique et sur l'utilisation des ressources informatiques m'est applicable.

J'ai lu le document susmentionné et m'engage à suivre toutes les directives et méthodes qui y sont énoncées. Je conviens également de me conformer à toutes les normes énoncées dans ce document pendant la durée de mon emploi (ou contrat) auprès de la Société.

Nom de l'employé : _____

Signature de l'employé :_____

Date : _____