POL 49-02
Politique sur la sécurité informatique
Direction Technologies de l'information

En vigueur : 2010-01-01	Approbation : Marc Tremblay Président-directeur-général Conseil d'administration
Révisé le :	

Palais
des congrès
de Montréal

Table des matières

1. Contexte

La Société du Palais des congrès de Montréal reconnaît que ses actifs informationnels, que sont l'ensemble des données et des équipements, contiennent l'information essentielle à ses activités et, de ce fait, qu'ils doivent faire l'objet d'une protection adéquate. La Société reconnaît que ses actifs informationnels contiennent, en outre, des renseignements personnels, des renseignements de nature confidentielle ainsi que des informations qui ont une valeur légale, administrative ou économique.

Dans la mesure où les actifs informationnels sous sa responsabilité doivent être protégés et sécurisés et afin de s'assurer du respect des lois, des normes et des règlements gouvernementaux, la Société met en place la présente politique de sécurité informatique qui oriente et détermine l'utilisation et l'encadrement appropriés et sécuritaires des actifs informationnels qu'elle possède.

2. Avis

La présente Politique sur la sécurité informatique remplace la Politique cadre sur l'utilisation acceptable des systèmes informatiques.

3. Objectifs

Cette politique vise à :

- Assurer la disponibilité, l'intégrité et la confidentialité de l'utilisation des réseaux et des applications informatiques, d'Internet et de l'intranet, permettant ainsi d'assurer la confidentialité des actifs informationnels et des données corporatives sensibles;

- Énoncer, faire connaître, mettre en place et appliquer les principes et les règles permettant d'assurer la sécurité, l'intégrité et le bon fonctionnement des systèmes informatiques;

- Défendre le respect de la vie privée des personnes, notamment, la confidentialité des renseignements à caractère nominatif relatifs au personnel de la Société, aux membres du conseil d'administration, à ses clients et à ses fournisseurs et partenaires;

- Sensibiliser et orienter tous les utilisateurs quant à leurs responsabilités dans la protection des actifs informationnels dont il faut assurer la confidentialité, l'intégrité et la disponibilité;

- Assurer la conformité aux lois et règlements applicables ainsi qu'aux directives, normes et orientations gouvernementales.

Cette politique s'accompagne de directives et de procédures afin de préciser les obligations qui en découlent.

4. Interprétation

Le président-directeur général, le directeur exécutif des opérations et des finances et le directeur des technologies de l'information peuvent fournir les interprétations requises concernant la présente politique.

5. Portée

La Politique de sécurité informatique s'adresse à l'ensemble du personnel de la Société. De plus, elle s'étend à toute personne physique ou morale qui utilise, pour le compte de la Société ou non, les actifs informationnels de la Société.

Elle s'adresse, enfin, à l'ensemble des actifs informationnels, à leur utilisation au sein de la Société ainsi qu'à l'ensemble des activités de collecte, d'enregistrement, de traitement, de garde, d'impression et de diffusion des actifs informationnels de la Société et principalement à toutes les applications qui recueillent, traitent et produisent des données financières.

6. Définitions

Aux fins de la présente politique, les termes suivants sont définis comme suit :

6.1 Actif informationnel

Tout équipement relié ou non au réseau, logiciel, système, donnée ou information utilisés pour l'hébergement, le traitement, la diffusion et l'échange d'information, acquis ou constitué par la Société.

6.2 Analyse et évaluation des risques

Analyse et évaluation des menaces, des impacts et des vulnérabilités auxquels l'information et les infrastructures de traitement de l'information sont exposées et de la probabilité de leur survenance.

6.3 Application

Un ensemble organisé de moyens informatiques (traitements, données et interfaces), incluant les progiciels, mis en place pour recueillir, traiter, emmagasiner, communiquer et éliminer l'information dans le but de répondre à un besoin déterminé et de supporter les processus de travail des utilisateurs.

6.4 Authentification

Un acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif.

6.5 Confidentialité

Une exigence en vertu de laquelle une information est divulguée, traitée et mise à la disposition des seules personnes ou entités autorisées, selon les modalités établies.

6.6 Contrôle d'accès

Une fonction permettant aux systèmes de contrôler l'accès aux ressources selon des autorisations préalablement définies.

6.7 Disponibilité

Une exigence en vertu de laquelle la propriété d'un actif informationnel est accessible et utilisable par une personne ou par une entité, dans les conditions autorisées.

6.8 Droit d'accès

Le droit d'utiliser un actif informationnel selon des modalités qui varient en fonction du niveau de privilège accordé.

6.9 Gestion des risques

Un processus d'identification, de contrôle et de réduction ou d'élimination des risques qui pourraient affecter les actifs informationnels, moyennant un coût acceptable.

6.10 Incident de sécurité informatique

Tout événement susceptible de contrevenir aux objectifs, aux règles et aux normes institutionnelles de sécurité informatique.

6.11 Intégrité

Une exigence se rapportant aux données ou aux systèmes. L'intégrité des données est une exigence qui veut que l'information et les programmes ne soient modifiés que d'une manière déterminée et autorisée, tandis que l'intégrité des systèmes est une exigence qui veut qu'un système remplisse les tâches auxquelles il est destiné, libre de toute manipulation non autorisée, qu'elle soit délibérée ou commise par inadvertance.

6.12 Mesure de sécurité informatique

Un moyen organisationnel, technologique, humain ou juridique permettant d'assurer la réalisation des objectifs de disponibilité, d'intégrité et de confidentialité de l'information ainsi que d'authentification des personnes et des dispositifs et de l'irrévocabilité des actions qu'ils posent.

6.13 Norme

Un accord documenté contenant des spécifications techniques ou autres critères précis destinés à être utilisés systématiquement en tant que règles, lignes directrices ou définitions de caractéristiques pour assurer que des matériaux, produits, processus et services sont aptes à leur emploi.

6.14 Relève informatique

Un ensemble des mesures de planification établies et appliquées en vue de rétablir une disponibilité adéquate des actifs informationnels indispensables à la réalisation de certaines activités.

6.15 Renseignement de nature confidentielle

Un renseignement qui ne doit pas être divulgué à des personnes non autorisées comme l'indiquent des dispositions de la Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels.

6.16 Renseignement personnel ou nominatif

Un renseignement qui concerne une personne physique et qui permet de l'identifier.

6.17 Responsable d'application

Tout service ou intervenant désigné responsable et imputable de la gestion de certains actifs informationnels de la Société. Cet actif peut consister en un actif complet ou en une portion (module) de cet actif.

6.18 Risque

Le degré d'exposition des actifs informationnels aux menaces, en fonction de la valeur de ces actifs et des mesures en place pour en préserver la sécurité.

6.19 Utilisateur

Toute personne de la Société de quelque catégorie d'emploi, de statut d'employé ayant accès à l'actif informationnel, ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement (par exemple : les fournisseurs des applications utilisées), accède à l'actif informationnel de la Société.

7. Énoncé des principes

La Société considère que la sécurité informatique doit être vue comme :

- Une démarche

elle se définit alors comme la poursuite active des objectifs de confidentialité, d'intégrité et de disponibilité de manière à ce que les actifs informationnels soient utilisables dans des conditions adéquates;

- Un objectif

elle se définit alors comme un objectif qui vise à maintenir les conditions adéquates pour que les actifs informationnels soient utilisables, dans le respect des exigences de confidentialité, d'intégrité et de disponibilité;

- un résultat

Elle se définit alors comme l'état des actifs informationnels qui sont utilisables dans de conditions adéquates, dans le respect des exigences de confidentialité, d'intégrité et de disponibilité.

La sécurité informatique est une responsabilité institutionnelle et personnelle de sorte que l'atteinte des objectifs de cette politique repose sur la reconnaissance et la mise en œuvre d'un ensemble de droits et de responsabilités individuelles qui respectent les principes directeurs suivants :

- le respect des droits des utilisateurs tels qu'ils sont définis dans la présente politique;

- l'analyse et l'évaluation des risques en matière de sécurité informatique;
- l'amélioration constante des mécanismes administratifs, préventifs et d'intervention pour permettre de poser les actions requises dans les situations mettant en péril la sécurité des actifs informationnels;

- la fiabilité, la qualité et le bon fonctionnement des services qui permettent à la Société de réaliser sa mission et ses objectifs, dans le respect des droits et libertés des personnes, ainsi que des lois et règlements;

- la recherche et la mise en œuvre de moyens afin de protéger le travail des personnes en permettant une utilisation des actifs informationnels dans des conditions optimales;

- la résolution des problèmes de sécurité informatique par une approche proactive et préventive plutôt que par une approche réactive;

- la sensibilisation des utilisateurs, en mettant les moyens nécessaires à leur disposition, à l'importance d'assumer les responsabilités préconisées par la politique de sécurité informatique, et ce considérant qu'ils sont les principaux artisans de la mise en application efficace d'une telle politique à la Société.

8. Droits et responsabilités

Tous les utilisateurs ont des droits quant à la sécurité informatique. Ces droits varient en fonction du ou des rôles que chacun est appelé à jouer dans l'utilisation et dans la gestion des actifs informationnels.

Ces droits visent à définir, du point de vue de la sécurité informatique uniquement, les attentes légitimes que les utilisateurs peuvent nourrir à l'égard des services offerts par la Société et ses représentants. Ceux-ci, dans le cadre de la gestion des actifs informationnels, ont donc le devoir de respecter ces droits dans toutes les décisions et actions entreprises.

Les utilisateurs ont également des responsabilités à l'égard de la sécurité informatique. Le respect de ses responsabilités permettra à chacun, selon son rôle, de contribuer à différents degrés à la sécurité des actifs informationnels. Ces responsabilités sont attribuées autant aux utilisateurs, qui par une saine utilisation des actifs informationnels assurent leur sécurité et leur stabilité, qu'aux gestionnaires de ces actifs, qui doivent mettre en place des mécanismes raisonnables pour les protéger dans le respect des droits des utilisateurs.

8.1 Droits et responsabilités des utilisateurs

Les droits et les responsabilités des utilisateurs sont applicables à l'ensemble des utilisateurs des actifs informationnels de la Société.

8.1.1 Droits

Les utilisateurs des actifs informationnels de la Société ont un droit d'accès à ces actifs, conforme à leur rôle et leur niveau de responsabilité dans l'organisation, ainsi que de préservation de la confidentialité de leur utilisation, sous réserve d'un manquement à la présente politique.

Les utilisateurs ont le droit d'avoir accès à des services informatiques fiables et disponibles, dans les limites de la capacité de la Société à leur fournir.

Les utilisateurs ont le droit d'être informés, sensibilisés et formés à l'égard de leurs responsabilités et de disposer des moyens (par exemple : des guides, des ressources humaines et financières, etc.) nécessaires à leur prise en charge.

La Société accorde un droit d'utilisation individuelle de ses actifs informationnels dans la mesure où celle-ci est conforme aux besoins liés à leurs tâches dans l'organisation.

Dans le cas où un utilisateur a besoin d'un accès supérieur aux normes institutionnelles prévues dans le cadre de cette politique, il

a le droit d'obtenir un tel accès à la condition qu'il ait été approuvé par les responsables des actifs informationnels utilisés.

8.1.2 Responsabilités

Les utilisateurs doivent respecter les directives prescrites dans le cadre de la présente politique et toutes autres directives et procédures existantes, en matière d'utilisation des actifs informationnels :

- en utilisant un mot de passe personnel, établi selon la directive en vigueur, pour gérer leurs accès aux actifs informationnels de la Société et en préservant la confidentialité et l'intégrité de ce mot de passe;

- en tenant compte des droits d'accès accordés ainsi que de leurs modalités d'utilisation afin de préserver l'intégrité et la disponibilité des actifs informationnels;

- en respectant les droits d'accès tel que prévu lors de l'octroi;

- en assurant la protection des actifs informationnels sous leur responsabilité;

- en ayant recours aux actifs informationnels de la Société conformément au cadre législatif auquel la Société est soumise.

Dans le cas de l'octroi d'un privilège temporaire, l'utilisateur doit limiter son utilisation des actifs informationnels de la Société aux modalités prescrites dans le cadre de cette autorisation.

Outre ces responsabilités, les utilisateurs doivent prendre connaissance des consignes de sécurité informatique qui sont portées à leur attention et agir conformément aux recommandations pertinentes lorsqu'ils utilisent les actifs informationnels.

De plus, les utilisateurs qui constatent un incident de sécurité informatique devraient poser les actions appropriées, selon la nature de l'incident, pour corriger la situation et limiter les probabilités qu'il survienne de nouveau. Dans la mesure où les utilisateurs jugent qu'ils ne disposent pas des moyens pour poser les actions correctives nécessaires, ils devraient signaler, dans les meilleurs délais, l'incident au responsable de la sécurité informatique.

Les utilisateurs devraient également collaborer, dans la limite où cette collaboration ne leur porte pas un préjudice personnel, avec les services appropriés dans le cadre des exercices d'évaluation de la sécurité informatique et des investigations d'incidents de sécurité informatique.

8.2 Droits et responsabilités du personnel cadre

8.2.1 Droits

Outre les droits et responsabilités dévolus à tous les utilisateurs, un employé agissant à titre de cadre a également le droit de faire une utilisation des actifs informationnels qui lui permettent d'exécuter les tâches propres à sa fonction de gestionnaire.

Le cadre a le droit d'être informé des incidents touchant l'application de la présente politique dans sa direction.

Dans l'un ou l'autre cas, il peut appliquer des mesures de sécurité informatique plus restrictives que celles définies dans les directives et procédures de sécurité informatique, s'il juge que ces restrictions sont requises par la nécessité de la direction et qu'elles respectent les principes de la politique de sécurité informatique.

De plus, un cadre a le droit, moyennant l'acceptation de modalités spécifiques d'utilisation et de gestion des actifs informationnels à leur charge, de déléguer certaines responsabilités de sécurité informatique au Service informatique ou à un responsable d'application.

8.2.2 Responsabilités

Un cadre s'engage à respecter la politique de sécurité informatique de la Société ainsi que toutes autres directives ou procédures existantes en matière d'utilisation des actifs informationnels.
Plus spécifiquement, un cadre est également responsable, avec le soutien du responsable de la sécurité informatique :

- d'identifier, en collaboration avec leur supérieur immédiat, les actifs informationnels dont il est responsable et de désigner au responsable de la sécurité informatique un ou des responsable(s) d'application;

- de préciser les besoins de sécurité informatique (confidentialité, intégrité et disponibilité) inhérents aux actifs informationnels dont il est responsable;

- de participer, en collaboration avec les responsables d'applications concernés, au processus d'autorisation et de gestion des accès informatiques conformément aux directives et procédures prévues à cet effet;

- de fournir un soutien aux activités d'identification des besoins de sécurité informatique, d'approbation des solutions proposées et de réalisation des tests de fonctionnalité dans le cadre du développement des projets technologiques, de la mise à jour ou de l'application d'un correctif d'un fournisseur d'application.

Cette personne doit mettre en place les mesures de sécurité informatique préconisées par la politique de sécurité informatique et toutes autres directives et procédures prévues à cet effet. Elle doit sensibiliser le personnel sous sa responsabilité aux différents aspects de la sécurité informatique. Dans l'éventualité où elle n'est pas en mesure de mettre en œuvre les mesures de protection requises, elle doit communiquer avec les ressources habilitées à lui offrir un soutien.

De plus, elle doit collaborer aux investigations en vue de résoudre les problèmes de sécurité informatique ayant pour cible des actifs informationnels de la Société.

Finalement, cette personne doit, au besoin, donner son appui au responsable de la sécurité informatique dans l'exercice de vérification de la sécurité informatique des actifs sous sa responsabilité, définir avec lui un plan d'action si des mesures correctives sont nécessaires et superviser sa mise en application.

8.3 Droits et responsabilités des responsables d'application

8.3.1 Droits

Outre les droits et responsabilités dévolus à tous les utilisateurs, les responsables d'application ont le droit, au même titre que tous les autres utilisateurs, de faire usage des actifs informationnels qui lui permettent d'exécuter les tâches inhérentes à leur emploi à la Société.

De plus, les responsables d'application ont le droit, moyennant l'acceptation de modalités spécifiques d'utilisation et de gestion des actifs informationnels sous leur responsabilité, de déléguer certaines responsabilités de sécurité au Service informatique.

8.3.2 Responsabilités

Les responsables d'application s'engagent à respecter la politique de sécurité informatique de la Société ainsi que toutes autres directives et procédures existantes en matière d'utilisation des actifs informationnels. Ces personnes sont également responsables, avec le soutien du responsable de la sécurité informatique :

- d'identifier, en collaboration avec leur supérieur immédiat, les actifs informationnels dont elles sont responsables;

- de définir les besoins de sécurité informatique (confidentialité, intégrité et disponibilité) inhérents aux actifs informationnels dont elles sont responsables;

- de mettre en place les mesures de protection nécessaires et, dans l'éventualité où elles ne disposent pas des moyens pour les mettre en œuvre, de communiquer avec les ressources habilitées à leur offrir un soutien à cet effet;

- d'élaborer, de tester et de maintenir à jour les procédures inhérentes à la planification de la relève informatique des équipements dont elles ont la responsabilité et de coordonner ces activités avec les directions concernés;

- d'élaborer et de coordonner des procédures d'autorisation et de gestion des accès informatique;

- d'informer et de former le personnel chargé d'appliquer les procédures;

- d'assurer le suivi et la révision annuelle des droits d'accès des utilisateurs aux applications dont elles sont responsables;

- de collaborer avec le responsable de la sécurité informatique afin d'établir les normes institutionnelles et mécanismes de protection nécessaires à la sécurité des actifs informationnels dont elles sont responsables et d'appliquer ces normes institutionnelles et mécanismes;

- d'assurer la continuité des activités informatiques grâce à une surveillance régulière des actifs informationnels dont elles sont responsables;

- de fournir un soutien aux activités d'identification des besoins de sécurité informatique, d'approbation des solutions proposées et de réalisation des tests de fonctionnalité dans le cadre du développement des projets technologiques;

- d'appliquer les mécanismes de contrôle lors de la mise à jour ou de l'application d'un correctif d'un fournisseur d'application (par exemple : preuve de test, autorisation etc.);

- d'encadrer, dans la mesure où les projets de développement informatique sont sous leur responsabilité, le processus de gestion de projet, de manière à ce que les besoins de sécurité informatique soient intégrés dans son élaboration même, à ce que le responsable de la sécurité informatique donne son approbation à la solution proposée, à ce que des tests des caractéristiques de sécurité soient effectués et à ce que la mise en place des modifications aux systèmes respecte les normes institutionnelles et les procédures de sécurité informatique.

Les responsables d'application doivent sensibiliser les utilisateurs qu'ils soutiennent sur les différents aspects de la sécurité informatique.

De plus, ils doivent collaborer aux investigations pour résoudre les problèmes de sécurité informatique ayant pour cible des actifs informationnels de la Société.

Finalement, ils doivent, au besoin, donner leur appui au responsable de la sécurité informatique dans l'exercice de vérification de la sécurité informatique des actifs sous leur responsabilité, définir avec lui un plan d'action si des mesures correctives sont nécessaires et superviser sa mise en application.

8.4 Droits et responsabilités du responsable du Service de sécurité

8.4.1 Droits

Dans le cadre de sa mission fondamentale de prévention et de protection des personnes et des biens, le responsable du Service de sécurité a un droit d'utilisation prioritaire des systèmes informatiques essentiels à la préservation immédiate de la sécurité des personnes et des biens.

De plus, le responsable du Service de sécurité a le droit d'être informé des incidents de sécurité informatique se rapportant aux personnes, aux biens ou aux équipements, étant donné l'impact

qu'ils ont sur l'atteinte même de sa mission de préservation de la sécurité des personnes et des biens.

8.4.2 Responsabilités

Le responsable du Service de sécurité doit coordonner les tâches suivantes :

- planifier et coordonner avec le responsable de la sécurité informatique la gestion de crises informatiques et assurer la continuité des services tout en veillant à la sécurité des personnes et des biens;

- fournir un soutien au Service informatique dans le cadre des enquêtes de sécurité informatique et coordonner les interventions d'organismes externes en charge de la protection publique;

- assister les responsables d'application dans le choix et la mise en œuvre des mesures de protection nécessaires pour assurer la sécurité physique des actifs informationnels.

8.5 Droits et responsabilités du personnel du Service informatique

8.5.1 Droits

Dans le cadre de sa mission fondamentale de prestation de services informatiques, le Service informatique a le droit de prendre les mesures nécessaires pour protéger les actifs informationnels sous sa responsabilité. Dans un contexte de mesures d'urgence ou de plaintes, il a également un droit de circonscrire l'accès à tout actif informationnel qui peut avoir une incidence sur la prestation des services qu'il soutient.

Le Service informatique a le droit, pour des motifs raisonnables et après avoir obtenu l'autorisation du directeur exécutif aux opérations et aux finances, de procéder à toutes les vérifications d'usage qu'il estime nécessaires pour s'assurer du respect des dispositions de cette politique ou des modalités d'utilisation prescrites lors de l'autorisation de l'accès aux actifs informationnels.

8.5.2 Responsabilités

Le Service informatique, en tant qu'unité organisationnelle, a la responsabilité de fournir à ses employés, dans la limite des ressources qui lui sont octroyées, les moyens nécessaires à la réalisation de leurs tâches de protection des actifs informationnels et de coordonner leur travail dans le cadre de la réalisation de ces tâches.

Le personnel du Service informatique, outre ses responsabilités à titre d'employé, de supérieur immédiat ou d'utilisateur des actifs informationnels, a certaines responsabilités spécifiques découlant de la mission du Service informatique en matière de prestation de services informatiques. Ainsi, le Service doit offrir ou soutenir les activités suivantes, tout en s'assurant que les utilisateurs soient mis au courant et, au besoin, formés :

- identifier, en collaboration avec leur supérieur immédiat, les actifs informationnels dont il est responsable et désigner un ou des responsable(s) d'application en mesure de répondre au responsable de la sécurité informatique;

- analyser et évaluer les risques et besoins en matière de sécurité informatique (confidentialité, intégrité et disponibilité) inhérents aux actifs informationnels dont il est responsable;

- mettre en place les mesures de protection nécessaires et, dans l'éventualité où il ne dispose pas des moyens pour les mettre en œuvre, communiquer avec les ressources habilitées à offrir un soutien à cet effet;

- assurer la continuité de service des actifs informationnels sous sa responsabilité en mettant en place des mesures de protection préventives ainsi que des procédures d'urgence en cas d'incidents;

- préserver la pérennité des actifs informationnels les plus importants en offrant aux responsables d'application certaines modalités de service de copies de sauvegarde;

- consolider la sécurité des actifs informationnels en définissant des procédures d'authentification, d'autorisation, de gestion et de contrôle des accès;

- établir, en collaboration avec le responsable de la sécurité informatique, les normes institutionnelles et mécanismes de protection nécessaires à la sécurité des systèmes et voir à leur application;

- participer à l'élaboration d'un plan de relève informatique et aux tests périodiques;

- participer au processus de gestion des dérogations à la politique de sécurité informatique, ainsi qu'aux directives et procédures de sécurité informatique établies;

- collaborer à l'investigation et au traitement des incidents ou problèmes de sécurité informatique;

- assurer la révision annuelle des comptes utilisateurs;

- encadrer les projets technologiques dont il a la charge, de manière à ce que les besoins de sécurité informatique soient intégrés dans leur élaboration même et à ce que la solution proposée soit approuvée et veiller également à ce que des tests de caractéristiques de sécurité soient effectués et à ce que la mise en place des modifications aux systèmes soit sécuritaire;

- assurer la continuité des activités informatiques en procédant à une surveillance régulière (continuité des opérations, incidents de sécurité, niveau de service, etc.) des actifs informationnels dont le service est responsable.

8.6 Droits et responsabilités du responsable de la sécurité informatique

Le mandat du responsable de la sécurité informatique consiste à :

- assurer aux utilisateurs une utilisation et une gestion sécuritaires, responsables et éthiques des actifs informationnels;

- sensibiliser et orienter chacun des utilisateurs quant à ses responsabilités dans la protection des actifs informationnels dont il faut assurer la confidentialité, l'intégrité et la disponibilité.

8.6.1 Droits

Le responsable de la sécurité informatique, outre ses droits à titre de membre du personnel du Service informatique, peut procéder à une évaluation des risques informatiques d'une application de la Société et formuler des recommandations aux utilisateurs quant aux meilleures pratiques de protection des actifs informationnels.

Le responsable de la sécurité informatique peut, dans le cadre de ses fonctions, ou par mandat, procéder au contrôle de la conformité des actifs informationnels et des procédures appliquées avec les normes institutionnelles de sécurité en vigueur, dans le but d'informer le comité de direction des risques encourus par ses actifs.

Il est également habilité à enquêter dans les cas d'incidents de sécurité informatique, à coordonner la résolution des problèmes et la stratégie de communication, ainsi qu'à représenter la direction de la Société dans le cadre des activités courantes se rapportant à la sécurité informatique, tout en respectant les mandats propres à la Direction des ressources humaines, à la Direction du marketing et des communications et au Service de sécurité.

Outre ces droits spécifiques, le responsable de la sécurité informatique a les droits nécessaires à l'exercice des responsabilités qui lui sont attribués dans le cadre de la protection des actifs informationnels.

8.6.2 Responsabilités

Outre les responsabilités à titre de membre du personnel du Service informatique, le responsable de la sécurité informatique a notamment les responsabilités spécifiques suivantes découlant de son poste :

- mettre en œuvre des mécanismes de sensibilisation, d'information et de formation (groupes d'intérêts, comités, etc.) visant à assurer une meilleure diffusion des enjeux et des connaissances se rapportant à la protection des actifs informationnels;

- consolider l'inventaire des actifs informationnels communiqué par les responsables d'application;

- soutenir le personnel cadre, les responsables d'application et le Service informatique dans l'évaluation des risques technologiques et des besoins de sécurité informatique inhérents aux actifs informationnels de la Société;

- assurer une veille stratégique des vulnérabilités et opportunités d'amélioration de la sécurité informatique;

- protéger les actifs informationnels de la Société en définissant des politiques, des directives et des procédures relatives à la sécurité informatique et en vérifiant la conformité des pratiques avec ces règles;

- développer, mettre à jour et diffuser des programmes de sensibilisation et de formation à l'égard de la sécurité informatique;

- coordonner l'élaboration d'un plan de relève informatique et procéder à des tests planifiés périodiques;

- coordonner les équipes d'intervention ponctuelles requises en cas de crise de sécurité informatique;

- établir et coordonner le processus de gestion des incidents informatique, comportant leur inscription dans un registre formel, leur classification et le suivi systématique de tous les incidents informatiques pour permettre leur traitement uniforme et la gestion des priorités des interventions;

- investiguer tous les cas d'incidents de sécurité informatique qui lui sont rapportés et coordonner la résolution des problèmes et la communication avec les directions concernées;

- coordonner la révision annuelle des comptes utilisateurs et des droits d'accès;

- établir et réviser annuellement les droits d'accès spéciaux accordés aux administrateurs de systèmes;

- établir et assurer le suivi de mécanismes de contrôle relativement aux interventions effectuées par les détenteurs de droits d'accès spéciaux;

- participer aux différents projets technologiques afin d'harmoniser les aspects de sécurité informatique;

- établir les mécanismes de contrôle et s'assurer que la mise à jour ou l'application d'un correctif d'un fournisseur d'application sont documentés (par exemple : preuve de test, autorisation, etc.);

- coordonner le processus de gestion des dérogations à la politique de sécurité informatique, ainsi qu'aux directives et aux procédures de sécurité informatique établies;

- coordonner et suivre la mise en œuvre de toute recommandation découlant d'une vérification ou d'un audit;

- produire trimestriellement, et au besoin, les bilans et les rapports relatifs à la sécurité des actifs informationnels appartenant à la Société, dont les incidents informatiques, en s'assurant que l'information sensible à diffusion restreinte est traitée de manière confidentielle et les soumets au directeur exécutif des opérations et des finances, au comité de direction et au comité de vérification.

8.7 Droits et responsabilités du comité direction

8.7.1 Droits

À titre de responsable de la gestion courante, le comité de direction de la Société a le droit d'intervenir dans la gestion de la politique de sécurité informatique et d'en demander une révision au moment où elle le juge opportun, et ce, par l'entremise du directeur exécutif des opérations et des finances, à titre de supérieur immédiat du responsable de la sécurité informatique des actifs informationnels;

Le comité de direction de la Société a également le droit de mandater les directions appropriés pour mettre en place ou renforcer les mesures de sécurité informatique prescrites dans le cadre de la politique de sécurité informatique ou pour en évaluer le respect par les utilisateurs.

Le comité de direction de la Société possède également un droit de regard sur l'état de conformité de la protection des actifs informationnels de l'organisation avec la politique de sécurité informatique, et toutes autres directives et procédures existantes.

8.7.2 Responsabilités

Le comité de direction de la Société a, en ce qui a trait à la sécurité informatique, les devoirs spécifiques suivants :

- approuver les évaluations de risques qui lui sont soumises ainsi que les plans d'action s'y rattachant;

- fournir un soutien formel aux mesures proposées de sécurité informatique qu'elle approuve;

- statuer, à la suite des recommandations des utilisateurs concernés, sur les demandes de dérogation aux politiques, aux directives et aux procédures qui font l'objet d'un litige aux instances inférieures;

- approuver et revoir, au besoin, la politique de sécurité informatique et les directives s'y rattachant;

- d'établir et de revoir périodiquement les mesures disciplinaires à imposer dans les cas de non-conformité ou de violation de la politique de sécurité informatique ou des directives s'y rattachant.

9. Procédures découlant de la politique de sécurité informatique

9.1 Sensibilisation, information et formation

La Société, par l'adoption, la diffusion et la mise en œuvre de la politique de sécurité informatique, amorce la sensibilisation de tous les utilisateurs aux principes énoncés dans la présente politique.

Tout utilisateur a le droit de recevoir les renseignements nécessaires à la bonne compréhension de ses responsabilités en matière de sécurité informatique. À cet effet, il pourra notamment avoir accès à des documents explicatifs et à des formations.

Les modalités de formation et de communication devront être convenues entre les individus concernés, selon les disponibilités respectives des participants et les modes de formation jugés les plus efficaces.

Les communications concernant la sécurité informatique pourront être effectuées par le biais de plusieurs canaux de communication selon l'auditoire, l'objet et l'urgence de la communication.

Tout utilisateur est responsable de consulter régulièrement les canaux de communication mis à sa disposition à la Société (boîte de courriels, boîte vocale, avis imprimés, intranet, etc.), afin de prendre connaissance des informations pertinentes se rapportant à la sécurité informatique.

Tout utilisateur a le droit de demander aux responsables d'application, au Service informatique ou au responsable de la sécurité informatique, des explications ou des renseignements supplémentaires quant aux modalités d'utilisation, de gestion et de protection des actifs informationnels. Il peut le faire dans la mesure où les renseignements demandés ne compromettent pas la sécurité même des actifs. À la suite de la réception d'une demande légitime, le responsable d'application, le Service

informatique ou le responsable de la sécurité informatique doit fournir l'information demandée dans les meilleurs délais possibles.

9.2 Traitements des incidents

9.2.1 Mesures d'urgence

Dans le cas d'événements requérant une intervention d'urgence pour protéger la confidentialité, l'intégrité ou la disponibilité d'actifs informationnels, toute personne témoin d'un incident doit informer le Service informatique ou lui confier le cas afin qu'il coordonne les interventions de sécurité informatique, en concertation avec le directeur exécutif des opérations et des finances et les autres directeurs concernés.

Afin de préserver l'intégrité du service, le Service informatique peut, après avoir pris les moyens raisonnables pour aviser les responsables ou les utilisateurs des actifs informationnels, poser les actions suivantes :

- interrompe ou révoquer temporairement les services offerts à certains utilisateurs afin de protéger le reste des utilisateurs, en tentant le plus possible de restreindre l'accès qu'au service qui pose le problème;

- intervenir sur un actif informationnel suspecté de contrevenir à la politique de sécurité informatique, aux directives ou aux lois et, au besoin, demander à la personne l'utilisant de s'identifier;

- appliquer les différentes fonctions de diagnostic sur les actifs informationnels;

- mettre en place les mesures urgentes requises afin de circonscrire la crise.

9.2.2 Communication et traitement des incidents

Les personnes qui constatent un incident de sécurité doivent prendre les actions appropriées à la nature de l'incident pour corriger la situation et limiter les probabilités qu'il survienne de nouveau. Dans la mesure où les utilisateurs jugent qu'ils ne sont pas en mesure de poser les actions correctives, ils doivent rapporter, dans les meilleurs délais, l'incident au responsable de la sécurité informatique.

Chaque incident rapporté fera ensuite l'objet d'un suivi auprès des directions et des personnes concernées pour examen, communication des résultats pertinents et proposition de mesures correctives.

9.2.3 Sanctions

Dans le cas où des incidents de sécurité informatique résulteraient d'agissements volontaires et malicieux d'un utilisateur, celui-ci est passible de mesures disciplinaires, prévues par la Politique des mesures disciplinaires de la Société, en fonction de la gravité et de la répétition des gestes posés par l'utilisateur fautif. Ces mesures seront appliquées selon les modalités prévues aux conventions collectives, dans le cas des employés syndiqués de la Société.

9.3 Processus de dérogation

9.3.1 Demande

Toute situation nécessitant un assouplissement de la politique de sécurité informatique, des directives ou procédures y afférents, une demande de dérogation doit être formulée par écrit auprès du responsable de la sécurité informatique.

9.3.2 Approbation des dérogations

L'approbation des dérogations aux dispositions de la politique de sécurité informatique, des directives ou des procédures y afférents est la responsabilité du responsable de la sécurité informatique. Cette approbation sera accordée à la suite de l'étude de la demande par les différents intervenants concernés (par exemple : le service informatique, le responsable de la sécurité informatique, le requérant ou le directeur du service requérant).

Dans l'éventualité d'un désaccord entre le requérant et le responsable de la sécurité informatique, le requérant peut présenter une demande de révision au comité de direction de la Société, par l'entremise du directeur exécutif des opérations et des finances qui déterminera de la pertinence d'une telle démarche.

9.4 Gestion, mise à jour et mise en œuvre de la politique informatique

9.4.1 Élaboration et révision

L'élaboration et la révision de la politique de sécurité informatique sont sous la responsabilité du directeur exécutif des opérations et des finances en collaboration avec le responsable de la sécurité informatique.

9.4.2 Adoption et date d'entrée en vigueur

L'approbation de la politique de sécurité informatique et des modifications qui devraient y être apportées relève du conseil d'administration de la Société. La présente politique entre en vigueur à la date de son approbation par le conseil d'administration de la Société. Il en est de même de toute modification à cette politique.

9.4.3 Adhésion

L'implantation et l'efficacité d'une politique de sécurité informatique au Palais des congrès de Montréal requièrent de la part de tous les utilisateurs le respect des pratiques et des procédures de sécurité informatique.

Les personnes qui sont appelées à jouer différents rôles au sein de la Société, conformément aux définitions présentées dans les sections 5 et 6 de la présente politique, s'engagent à assumer les responsabilités relatives aux fonctions qu'ils occupent.

9.4.4 Responsabilité de mise en œuvre

Dans le cadre de la mise en œuvre et de l'application de la politique de sécurité informatique, des directives et des procédures y afférents, le chef de service, informatique agit à titre de responsable de la sécurité informatique.

Le responsable de la sécurité informatique doit développer les mécanismes de soutien à la diffusion et à la mise à jour de la politique informatique.

La mise en œuvre et le respect de la présente politique et des directives ou des procédures en découlant incombent à tous les utilisateurs des actifs informationnels de la Société.

Le personnel cadre de chaque service doit sensibiliser son personnel et autres utilisateurs des actifs informationnels dont il est responsable, à l'importance des principes de sécurité entourant leur usage.

La Société est responsable de fournir les ressources nécessaires aux utilisateurs et au personnel cadre afin qu'ils puissent assumer leurs responsabilités quant à la sécurité informatique, et ce, dans un cadre de saine gestion des risques.