

POL 49-01  
Politique sur l'utilisation acceptable des systèmes  
informatiques  
Direction Technologies de l'information

En vigueur : 2004-02-09	Approbation : Paul Saint-Jacques Président-directeur-général
Révisé le :	

## Table des matières

<b>1</b>	<b>Objet</b> .....	<b>3</b>
<b>2</b>	<b>Objectifs</b> .....	<b>3</b>
<b>3</b>	<b>Interprétation</b> .....	<b>3</b>
<b>4</b>	<b>Portée</b> .....	<b>3</b>
<b>5</b>	<b>Dispositions générales</b> .....	<b>3</b>
5.1	Utilisation générale et propriété .....	3
5.2	Sécurité et information exclusive .....	4
5.3	Utilisation inacceptable .....	5
5.3.1	<i>Activités relatives au système et au réseau</i> .....	5
5.3.2	<i>Activités relatives aux courriels ou aux communications</i> .....	7
<b>6</b>	<b>Sanctions</b> .....	<b>8</b>
<b>7</b>	<b>Définitions</b> .....	<b>8</b>
<b>8</b>	<b>Historique de la révision</b> .....	<b>9</b>



## 1 Objet

La présente politique a pour objet de mettre en place les principes et les règles concernant l'utilisation appropriée des systèmes informatiques afin de protéger les employés et les partenaires de la Société du Palais des congrès de Montréal et de prémunir cette dernière contre toute action illégale ou préjudiciable de la part d'individus ou d'organisations.

## 2 Objectifs

Cette politique vise à :

- Protéger le réseau informatique de la Société;
- Établir des règles de sécurité et faire en sorte que les utilisateurs s'y conforment;
- Limiter les risques encourus par la Société contre, notamment, les attaques virales, les atteintes à la sécurité des systèmes, les services en réseau et les problèmes juridiques.

## 3 Interprétation

Le président-directeur général, le directeur aux Finances et à l'administration et le chef des Services informatiques peuvent fournir les interprétations requises concernant la présente politique sur l'utilisation acceptable des systèmes informatiques appartenant à la Société.


## 4 Portée

La Politique cadre sur l'utilisation acceptable des systèmes informatiques s'adresse aux employés réguliers et temporaires, aux employés à l'événement, aux sous-traitants et aux consultants travaillant pour la Société, ainsi qu'à toutes les personnes branchées, directement ou indirectement, sur les systèmes de la Société.

## 5 Dispositions générales

### 5.1 Utilisation générale et propriété

- a) Bien que la Société désire préserver la vie privée de manière raisonnable, les données inscrites sur ses systèmes informatiques demeurent sa propriété. La Société ne peut donc pas garantir la confidentialité de l'information emmagasinée sur son réseau et dans ses appareils informatiques;



b) Les utilisateurs doivent faire preuve de jugement à l'égard du caractère raisonnable de l'utilisation personnelle qu'ils font des ordinateurs, des appareils et du réseau à leur disposition. Chaque service doit établir des directives claires concernant l'utilisation personnelles de l'Internet (Internet, Intranet, Extranet). En l'absence de directives, les utilisateurs observeront celles préconisées par les Services informatiques. En cas d'incertitude, les utilisateurs doivent se référer à leur gestionnaire respectif;

c) Toute information confidentielle de haute importance ou dont l'utilisation malveillante pourrait nuire aux activités de la Société doit être chiffrée (encryptée);

d) À des fins de sécurité et de maintenance, le personnel autorisé peut, à tout moment, surveiller l'équipement, les systèmes et l'utilisation du réseau;

e) La Société se réserve le droit de vérifier les réseaux et les systèmes informatiques afin de s'assurer du respect de la présente politique.

## 5.2 Sécurité et information exclusive

a) Les employés doivent prendre les mesures nécessaires pour empêcher l'accès non autorisé à des applications ou à des fichiers à utilisation restreinte;


- Exemples d'information confidentielle :  
information particulière sur l'organisation, stratégies de la Société, information sur les concurrents, secrets commerciaux, spécifications, listes de clients et données de recherche;

b) Les utilisateurs doivent protéger leurs mots de passe et ne pas partager les comptes :

- Les mots de passe des administrateurs (Services informatiques) et les mots de passe des utilisateurs doivent être respectivement modifiés tous les trimestres et tous les semestres;

c) Tous les ordinateurs personnels, les portables et les postes de travail doivent être dotés d'un économiseur d'écran protégé par un mot de passe jumelé à une fonction d'activation automatique établie, au plus, à quinze (15) minutes de pause;

d) L'information contenue dans les portables étant plus vulnérable, elle doit faire l'objet d'une protection particulière;



e) Des messages envoyés par des locuteurs à partir d'une adresse électronique de la Société à des groupes de discussions devraient contenir un avertissement indiquant que les opinions exprimées sont strictement personnelles et ne reflètent pas nécessairement la position de la Société, à moins que la participation à ces groupes ne fasse partie des attributions de l'emploi;

f) Tous les ordinateurs connectés aux systèmes d'Internet, d'Intranet et d'Extranet de la Société, qu'ils appartiennent à la Société ou non, doivent régulièrement exécuter un balayage de détection des virus avec un logiciel comprenant une base de données à jour;

g) Les utilisateurs doivent faire preuve d'une grande prudence lorsqu'ils ouvrent les pièces jointes de courriels expédiés par des inconnus et susceptibles de contenir des virus, des bobards ou un cheval de Troie.

### 5.3 Utilisation inacceptable


Généralement, les activités décrites ci-dessous sont interdites. Certains utilisateurs peuvent être exemptés de ces restrictions dans le cadre d'activités inhérentes à leurs postes (par exemple, l'administrateur des systèmes pourrait désactiver l'accès au réseau d'un ordinateur, si ce dernier perturbe les activités des autres).


En aucun cas un employé de la Société n'est autorisé à exercer une activité illégale ou en contradiction avec les lois locales, provinciales, fédérales ou internationales en utilisant des ressources appartenant à la Société.

La liste ci-dessous n'est pas exhaustive, mais tente d'encadrer les activités entrant dans la catégorie des utilisations inacceptables. Donc, les activités détaillées aux points 5.3.1 et 5.3.2 sont strictement interdites, sans aucune exception :

#### *5.3.1 Activités relatives au système et au réseau*


a) La violation des droits de toute personne ou de toute organisation protégée par les droits d'auteur, de secret commercial, de brevet ou de certaine propriété intellectuelle ou les lois et les règlements semblables, y compris, entre autres, l'installation et la distribution de logiciels « piratés » ou autres pour lesquels la Société ou l'utilisateur final ne détient pas de licence active;

- 
- b) La copie sans autorisation d'un produit protégé par le droit d'auteur, y compris, entre autres, la numérisation et la distribution de photographies de magazines, de livres ou d'autres sources protégées par le droit d'auteur, la musique protégée par le droit d'auteur, ainsi que l'installation de tout logiciel protégé par le droit d'auteur pour lesquels la Société ou l'utilisateur final ne détient pas de licence active;
  - c) L'exportation illégale de logiciels, d'information technique ou d'une technologie de chiffrement (encryptage) contrevenant à des lois régissant le contrôle de l'exportation internationale ou régionale. Les membres compétents de la direction devraient être consultés avant l'exportation de tout matériel informatique ou technologique;
  - d) L'introduction de programmes malveillants dans le réseau ou les serveurs (exemple : virus, vers, chevaux de Troie, bobards, etc.);
  - e) La divulgation d'un mot de passe à d'autres personnes ou la permission à des personnes non autorisées d'accéder et d'utiliser le compte d'un employé, notamment dans le cas de travail accompli à domicile;
  - f) L'utilisation de matériel informatique de la Société afin de participer activement à l'obtention ou à la transmission de matériel contrevenant aux lois et aux politiques en vigueur relativement au harcèlement sexuel ou au milieu de travail;
  - g) L'offre frauduleuse de produits, d'articles ou de services provenant de tout compte de la Société;
  - h) La création de brèches de sécurité ou de ruptures du réseau de communication. Les brèches de sécurité comprennent, entre autres, l'accès à des données dont l'employé n'est pas le destinataire prévu ou l'ouverture de session sur un serveur ou dans un compte pour lequel l'employé ne détient pas d'autorisation d'accès expresse, à moins que ces tâches ne fassent partie de ses attributions régulières. Aux fins de la présente section, « rupture » comprend, entre autres, le reniflage du réseau, l'inondation soudaine, la mystification de paquets, le déni de service et les fausses informations d'adresse à des fins malveillantes;
  - i) Le balayage (scanner) des ports ou de sécurité, à moins d'en avoir reçu la permission des Services informatiques;

- 
- j) L'exécution de toute forme de surveillance de réseau afin d'intercepter des données non dirigées vers l'ordinateur d'un employé, à moins que cette activité ne fasse partie de l'emploi ou du travail de l'employé;
  - k) L'accès à tout ordinateur, réseau ou compte en évitant les étapes d'authentification de l'utilisateur ou en déjouant les dispositifs de sécurité;
  - l) La perturbation ou le refus de service à tout utilisateur autre que l'ordinateur de l'utilisateur (exemple : une attaque pour déni de service);
  - m) L'utilisation de tout programme, script, commande ou envoi de messages divers dans l'intention de perturber ou de désactiver la session d'un utilisateur, et ce, localement ou par l'intermédiaire d'Internet, d'Intranet ou d'Extranet;
  - n) La divulgation de renseignements sur les employés de la Société à des parties externes.

#### 5.3.2 *Activités relatives aux courriels ou aux communications*

- a) L'envoi de courriels non souhaités, y compris des pourriels ou d'autres publicités à des personnes qui ne les ont pas précisément demandés (pollupostage);
- b) Toute forme de harcèlement et de communications à contenu diffamatoire pour la Société et ses membres par courriel, téléphone ou téléavertisseur, que ce soit dans le langage, la fréquence ou la taille des messages;
- c) L'utilisation non autorisée ou la contrefaçon de l'information contenue dans les entêtes des courriels;
- d) La sollicitation de courriels pour toute autre adresse de courriel que celle de l'expéditeur, dans l'intention de harceler ou de recueillir des réponses;
- e) La création ou l'acheminement de lettres dites « boules de neige », de « combines de Ponzi » ou d'autres opérations pyramidales de n'importe quel type que ce soit;
- f) L'utilisation, à l'intérieur de la Société ou dans tout service relié au réseau de la Société, de courriels non sollicités à des fins publicitaires ou autres;



g) L'envoi de messages non reliés au travail à un grand nombre d'utilisateurs du courriel de la Société;

h) L'envoi de messages non reliés au travail à un grand nombre de groupes de discussion du réseau Usenet (pourriel de groupes de discussion).

## 6 Sanctions

Tout employé qui enfreint cette politique peut être passible de mesures disciplinaires allant jusqu'au renvoi.

## 7 Définitions

Terme	Définition
<i>Pourriel</i> : non autorisés ou non	Diffusion massive de messages électroniques sollicités.
<i>Pollupostage</i> :	Pourriel à grande échelle.
« Reniflage » du réseau ( <i>sniffer</i> ) :	Logiciel qui tente de détecter les spécificités des réseaux.
Combine de Ponzi : recueillir des fonds pour	Arnaque populaire sur Internet consistant à des œuvres inexistantes.
Inondation soudaine :	Tactique de déni de service.
Mystification de paquet ( <i>spoofing paquet</i> ) :	Remplacement d'une partie des données d'un message par d'autres données inexactes.
Déni de service : totalement un réseau.	Attaque informatique concertée qui bloque
Lettre « <i>boule de neige</i> » :	Lettre de type pyramidale.
Virus :	Programme informatique malicieux.
Bobard :	Canular véhiculé par courriel.
Cheval de Troie :	Logiciel qui effectue un téléchargement invisible afin de détourner des données confidentielles vers l'extérieur.





## 8 Historique de la révision

- Diffusion restreinte de la politique pour fins de consultation, de validation et d'amendement :
  - Roch Magnan, le 3 novembre 2003.
- Révision corrective :
  - Roch Magnan, André Saucier, le 11 novembre 2003.
- Adoption par le comité de direction du 11 décembre 2003 :
  - Diffusion : Le 9 février 2004;
  - Entrée en vigueur : Le 9 février 2004.