Technologies de l'information

Directives de sécurité corporative

Département TI
Version 1.2
Mars 2014

Historique du document

Version	Date	Auteur	Description des modifications
1.0	05.02.2014	M.Gaudreau	Brouillon
1.1	31.03.2014	M.Gaudreau	Ajout des corrections suite à la révision du CD
1.2	07.05.2014	M.Gaudreau	Révision sur la récupération des courriels

Document statut et approbation

Statut	Approbation
Approuvé	Nom : Antoine Camarda Jean-Guy Cadorette Jean-Pierre Azzopardi
	Fonction : Membres du comité de direction
	Date : 31 mars 2014

Liste de distribution

A	Cc:
Tous les employés du Groupe Helios	

INDEX

Initiales _____

1. MOT DU PRÉSIDENT

La technologie et les actifs informationnels sont essentiels aux opérations du Groupe Helios et ses unités d'affaires. Elles doivent faire l'objet d'une utilisation appropriée et d'une protection adéquate. Le Groupe Helios détient des renseignements personnels ainsi que des informations qui ont une valeur légale, administrative ou économique. Leur utilisation doit être réglementée afin d'éviter des incidents qui pourraient avoir des conséquences fâcheuses autant pour l'employé, l'organisation ainsi que pour les gens qui bénéficient des services offerts par celle-ci. La présente directive vise à assurer le respect des lois, des règlements ou autres textes normatifs à l'égard de l'usage et du traitement de l'information et de l'utilisation des technologies de l'information et des télécommunications par les employés du Groupe Helios. Plus spécifiquement, l'organisation vise à assurer le respect de la vie privée des individus, notamment la confidentialité des renseignements à caractère nominatif relatifs aux clients et aux employés et à protéger les actifs informationnels détenus par l'organisation selon leur degré de sensibilité.

Le Groupe Helios exige de tout employé qui utilise les systèmes et les actifs informationnels de l'organisation ou qui a accès à de l'information, de se conformer aux dispositions de la présente directive.

Initiales _____

1.1 Introduction

L'information est plus que jamais au cœur des solutions permettant d'optimiser les processus d'affaires. En contrepartie, la sécurité des informations risque d'être compromise si des actions préventives et concrètes ne sont pas systématiquement entreprises lors de l'élaboration des solutions d'affaires électroniques ou lors de l'adoption de pratiques de gestion documentaire et de leur évolution tout au long de leurs cycles de vie. Pour ne mentionner que la fuite d'une information critique sur un projet d'importance, une opération comptable frauduleuse à l'aide d'un système informatique ou une attaque du cyberespace mettant en péril les opérations du groupe Helios, les risques sont multiples. Ces risques d'affaires à l'égard de la sécurité des informations peuvent être de nature légale, stratégique ou financière, peuvent entacher la réputation du groupe Helios et nuire au modèle de confiance de nos clients envers la compagnie.

L'importance de la protection des informations pour le groupe Helios justifie la mise en place d'un programme de gestion de la sécurité de l'information dans le but de maintenir les niveaux de risques en conformité aux attentes des dirigeants de l'entreprise. Ce programme doit aussi tenir compte des dimensions organisationnelles, humaines, juridiques, financières et technologiques.

Un programme efficient de sécurité de l'information nécessite une coordination et des actions concrètement intégrées provenant du haut de la hiérarchie vers le bas. L'endossement, la promotion, l'engagement formel ainsi que le soutien de la haute direction sont des préalables à la réussite du programme de sécurité de l'information. Ainsi, dans ce contexte, la présente directive est élaborée dans le but de soutenir un programme de sécurité de l'information chez le groupe Helios. Cette directive confirme l'engagement du groupe et démontre l'importance que revêt la protection de ses actifs informationnels.

Initiales _____

1.2 Objectif

Énoncer la directive corporative du groupe Helios afin **d'assurer l'intégrité, la confidentialité, la disponibilité de l'information et la protection de ses actifs informationnels**. Cette directive vise aussi à s'assurer que le groupe Helios sera en mesure de faire face à des défaillances techniques ou humaines, aux actes malveillants, ainsi qu'à des sinistres.

1.3 Définition

Information : information sous toute forme (écrite, alphanumérique, numérique, sonore, graphique, imagée, photographique, symbolique, dessinée, etc.), sur tout support médiatique ou canal de communication filaire et non-filaire.

Document : information organique et consignée, quel qu'en soit le support médiatique.

Système, technologies de l'information ou de communication : est considéré comme tel, notamment une base de données, une application, un programme, un logiciel, un équipement informatique ou de télécommunication, un espace virtuel, un ordinateur, une imprimante, un télécopieur, un téléphone, un émetteur radio, un numériseur, etc.

Actif informationnel : toute information, document, système et technologie de l'information ou de communication.

Responsable d'un actif informationnel : gestionnaire du groupe Helios agissant à titre de propriétaire ou de fiduciaire d'un actif informationnel.

Initiales _____

1.4 Principes généraux

La directive veut définir un ensemble de mesures à respecter visant la sécurité de l'information recueillie, détenue ou utilisée chez le groupe Helios. Outre le fait de protéger l'accès, le traitement, l'utilisation et la transmission de l'information, les principes généraux encadrant cette directive visent à ce que :

- Le groupe Helios puisse, via son représentant autorisé tel que défini ci-après, procéder à des vérifications de l'information résidant ou transitant sur le réseau ou sur ses équipements et ce, en tout temps et à son entière discrétion;
- Le département TI soit responsable de l'ensemble des mécanismes garantissant la sécurité des informations résidant sur tout support électronique;
- Le département TI fasse évaluer par un processus interne, sur une base régulière, les directives et les mécanismes de sécurité du groupe Helios face aux meilleures pratiques de sécurité;
- Seul le personnel autorisé puisse accéder et utiliser l'information raisonnablement nécessaire à son travail, selon les autorisations spécifiquement accordées;
- Le personnel ne divulgue pas l'information sans autorisation écrite de la personne visée par telle divulgation d'information ou des personnes parties à une entente de confidentialité (sauf exception prévue dans la *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., ch. P-39.1, dont vérification devra être faite auprès du secrétariat corporatif préalablement à toute divulgation non autorisée par la personne visée);
- L'information confidentielle mise à la disposition du personnel ne doit servir qu'à des fins professionnelles et pour le bénéfice du groupe Helios;
- L'utilisation de l'infrastructure ne doive servir qu'aux fins autorisées selon les directives en vigueur;
- Soient établis les mécanismes de respect et de sanctions des infractions à la directive.

Initiales _____

1.5 Champs d'application

Cette directive encadre toute information liée à l'ensemble des activités du groupe Helios et s'applique à toutes les unités.

Toute tierce partie, dont les services sont requis par le groupe Helios et ayant accès à de l'information confidentielle, est aussi soumise à la directive et elle doit s'engager par écrit à en respecter les normes, les procédures et les directives de sécurité qui lui sont connexes ou qui pourraient en découler.

1.6 Cadre réglementaire

Certains volets de la sécurité de l'information sont notamment régis par:

- La Loi concernant le cadre juridique des technologies de l'information (L.R.Q., chapitre C-1.1);
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., chapitre A-2.1);
- La Loi sur les archives (L.R.Q., chapitre A-21.1);
- La Loi canadienne sur le droit d'auteur (L.R.C., chapitre C-42);
- Le Code civil du Québec;
- La Loi sur la preuve (L.R.C., chapitre C-5);
- La Loi concernant le droit criminel (L.R.C. 1985, chapitre C-46);
- La Loi sur la sécurité civile (L.R.Q. chapitre S-2.3).

Initiales _____

1.7 Principes détaillés

Règles à observer et mesures à prendre

Responsabilités des employés et des gestionnaires

Le personnel du groupe Helios est responsable, dans le cadre de ses tâches et fonctions, de gérer efficacement l'accès, le traitement, l'utilisation et la protection de l'information, en fonction de sa nature, des ententes signées et de sa valeur, afin d'en assurer le caractère confidentiel.

Les gestionnaires responsables des unités qui recueillent, produisent, détiennent ou utilisent l'information sont responsables de fournir les autorisations prévues en vue de l'accès, du traitement et de l'utilisation de ladite information et en sont imputables.

Rôle du département TI

Tout amendement à la directive, toutes directives de sécurité ainsi que les procédures et normes qui en découlent doivent, préalablement à leur mise en application, avoir été révisés et approuvés par le département TI.
Le département TI s'assurera du niveau de sécurité, de son maintien et de sa mise à jour selon les meilleures pratiques en semblable matière.

Limitation dans la collecte d'informations

Dans le cas où la nature de l'information serait personnelle, seuls les renseignements nécessaires à l'exercice des activités du groupe Helios, et pour des fins raisonnables, devront être recueillis auprès de la personne visée ou, si la collecte est faite auprès d'un tiers, avec l'autorisation de la personne visée, le tout en conformité avec les dispositions de la *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., ch. P-39.1.

Classification et description

L'information doit être classifiée (classifications en annexe) en fonction de sa confidentialité, de sa disponibilité et de la durée de sa vie utile (à l'aide d'un calendrier de conservation).

Initiales _____

Mesures de sécurité

Des mesures de sécurité (ex. : chiffrement, contrôle d'accès, etc.) doivent être prises afin de protéger le caractère confidentiel de l'information.

Des mesures de sécurité (ex. : détection des virus informatiques, authentification manuelle ou signature électronique, pistes de vérification) doivent être prises pour préserver l'intégrité et l'authenticité de l'information, et afin de confirmer ou d'infirmer l'origine de l'information.

Des mesures de sécurité (ex. : copies, bureaux et classeurs sous clefs, mises en voûte externe, plans de continuité et plans de relève des technologies de l'information) doivent être prises afin d'assurer la disponibilité de l'information en cas de panne majeure ou de désastre.

Les mesures de sécurité doivent être adaptées au niveau de classification de l'information.

Conservation de l'information

L'information doit être conservée aussi longtemps qu'il est nécessaire, en fonction des besoins opérationnels de l'entreprise et des cadres réglementaires et/ou légaux applicables.

L'information qui n'a plus à être conservée doit être détruite selon les procédures établies dans le respect des règles de confidentialité.

Initiales _____

1.8 Mécanisme de suivi

La présente directive est émise pour toutes les unités. Les directions de ces unités feront un suivi de l'efficacité de la directive, en fonction des particularités de leur mission. À cette fin, elles implanteront les mécanismes suivants :

- Vérification régulière du respect des règles stipulées dans la directive et mise en place des encadrements qui en découlent, selon une planification qui tient compte des sujets à traiter en priorité. Des rapports sur le respect des règles stipulées dans la directive seront remis par le département aux gestionnaires responsables des unités visées sur une base régulière (mise en place projetée 2014).

- Révision annuelle des encadrements et des outils nécessaires à l'application de cette directive pour s'assurer qu'ils sont adéquats et pertinents selon l'évolution du contexte opérationnel, technologique, légal, etc.

- Programmes permanents d'information et de formation sur la directive et sur les encadrements qui en découlent.

- Consolidation et coordination des actions de suivi de la directive. Toutes les unités administratives doivent assurer l'application de la présente directive et fournir l'information nécessaire au suivi. Les mécanismes de suivi visent la mise en application et le respect des règles et principes de cette directive.

Initiales _____

2. PRINCIPES DIRECTEURS DE SÉCURITÉ TI

2.1 Responsabilités

Officier de sécurité (directeur TI)

L'officier doit s'assurer que les directives sont connues et respectées.
L'officier doit s'assurer que chacun connaît ses responsabilités.

Administrateurs

Les administrateurs doivent s'assurer de ne jamais divulguer les combinaisons et les accès qu'ils possèdent.
Les administrateurs sont responsables de maintenir les accès.
Les administrateurs sont responsables de surveiller les violations d'accès.
Les administrateurs doivent respecter la loi sur la confidentialité des informations.

Utilisateurs

Les utilisateurs doivent s'assurer de ne jamais divulguer les mots de passe qu'ils possèdent.

Chef de maintenance (site de Longueuil)

Le chef de maintenance est responsable en autre de fournir une ressource pour modifier la combinaison de la porte de la salle des serveurs lorsque demandé.

Responsables applicatifs (Power users)

Les responsables doivent s'assurer une fois par an que les accès aux applications sont valides.

Initiales _____

2.2 Mots de passe

Le mot de passe est l'une des principales façons de garantir la sécurité d'accès aux systèmes et à l'information de l'organisation. En conséquence, des précautions élémentaires s'appliquent :

- Utiliser un mot de passe d'au moins huit caractères, composé de lettres majuscules et minuscules, d'au moins un chiffre et un caractère spécial;
- Éviter d'utiliser un mot de dictionnaire ou un mot qui ressemble au nom de l'organisation, du service, du logiciel, du système ou de l'employé;
- Ne pas afficher ou écrire le mot de passe sur un papier à la vue d'autres personnes;
- Ne pas permettre à un intervenant d'ouvrir une session de travail sous l'identifiant de l'employé à moins d'avoir été formellement autorisé par le supérieur de ce dernier (l'employé est responsable des actions effectuées avec son identifiant et son mot de passe.);
- Verrouiller son poste de travail lorsqu'on quitte celui-ci pour une période déterminée ou momentanément;
- Changer le mot de passe à intervalles réguliers (maximum six mois) ou lorsque le système le demande est fortement conseillé;
- Ne divulguez en aucun temps vos mots de passe.

Entrer son mot de passe à chaque connexion à un site sécurisé est fortement conseillé. La fonction « *Me souvenir de mon mot de passe* » disponible dans les navigateurs ou dans certaines pages Web ne devrait pas être utilisée.

Votre nom d'utilisateur est gardé dans plusieurs transactions électroniques pour fins de vérification : c'est votre signature électronique. Selon le nombre de services que vous utilisez, vous pourriez avoir plusieurs noms d'utilisateurs et mots de passe à mémoriser. Le mot de passe est obligatoire pour tous les utilisateurs.

Pour les utilisateurs qui utilisent la prise de contrôle à distance d'ordinateur par le biais de <log me in, PC Anywhere> ou tout autre logiciel du même type, nous demandons d'utiliser un mot de passe complexe.

Pour ce faire, utilisez une paraphrase facile à retenir. Exemple; <Je me suis joint au Groupe Helios en janvier 2014> ce qui donne Jmsjaghej@2014

Initiales _____

2.3 Boîte vocale

Pas d'expiration du mot de passe.

2.4 Poste de travail (PC ou Portable)

La personnalisation (installation de progiciels ou autres) peut être effectuée par l'utilisateur à condition qu'il soit proprement licencié et qu'il soit relié à son travail. Il est fortement recommandé de coordonner avec le département TI.

Ainsi, le secteur TI s'assure de garder une copie légale de tous les logiciels installés. De plus, si on doit remplacer le poste de travail en cas de défectuosité, on aura tous les logiciels en main pour rebâtir le nouveau poste de travail.

Assurez-vous de verrouiller votre poste de travail si vous devez vous absenter. Un poste de travail déverrouillé et sans surveillance donne accès à toutes vos données sans difficulté.

Les PC doivent être protégés par un processus de mise en session. L'usager doit se mettre en session avec les serveurs Windows afin d'obtenir accès aux services informatiques.

Les PC doivent être protégés par un antivirus corporatif qui détecte également les « spyware / malware ».

Les PC reçoivent les mises à jour de sécurité toutes les semaines ou au besoin.

2.5 Copies de sécurité

Une copie de sécurité de vos fichiers situés sur les serveurs d'entreprise et de vos courriels est prise à tous les soirs. Les courriels détruits peuvent être restaurés dans un délai maximal de 14 jours.

La dernière version des fichiers est sauvegardée.

Notez qu'il n'y a pas de prise de copie des fichiers situés sur votre propre poste de travail, soit votre répertoire C, sauf si préalablement entendu avec le TI.

Initiales _____

2.6 Le plan de relève

Le plan de relève des TI vise tous les équipements informatiques et téléphoniques localisés dans les salles d'équipements situées à Longueuil et Montréal. Il couvre les trois crises suivantes :

- Salle des équipements inaccessible (relève immédiate);
- Bris d'équipement (relève maximale une semaine);
- Perte totale de la salle des équipements (relève en une semaine).

2.7 Les connexions à distance

Les accès via le Citrix ou VPN doivent être contrôlés par un niveau de sécurité, celui-ci étant contrôlé par la sécurité du réseau Windows.

Une encryption forte de type SSL (128 bits) est utilisée afin de protéger la confidentialité de l'information entre le poste client et le serveur VPN ou Citrix.

2.8 Les connexions à distance VPN (à-travers un Wireless Internet, Internet Hôtel ou Internet aéroport)

Les accès via un réseau sans fil dans les aéroports et les hôtels ne sont pas protégés par un pare-feu et par conséquent représentent un risque à la sécurité. L'utilisateur s'expose à une intrusion de son portable et, par conséquent, à la possibilité de donner accès par l'entremise de son portable à l'accès VPN. Un des risques potentiels est la prise de contrôle du portable sans autorisation et par le fait même d'avoir accès à toutes vos applications du groupe Helios.

Le portable doit être protégé par un coupe-feu lors de sa connexion sans fil au réseau Internet.

Initiales _____

2.9 Courriels reçus de l'Internet, interceptés et détruits

Par mesure de sécurité, certains courriels sont interceptés et détruits à la réception:

- les courriels contenant un virus détecté par notre logiciel d'anti-virus corporatif;
- les courriels en provenance d'un site reconnu pour envoyer des pourriels;
- les courriels en provenance d'un émetteur inconnu (émetteur ne s'étant pas identifié);
- les courriels ayant une mauvaise adresse (destinataire inconnu).

Le destinataire du courriel est avisé si le courriel a été intercepté et détruit.

Initiales _____

2.10 Utilisation personnelle de l'espace disque, du courriel et de l'Internet

RAISON D'ÊTRE

La présente directive vise à établir les règles d'utilisation par les employés du groupe Helios du courrier électronique (interne et externe) et de l'Internet. Les employés s'engagent et consentent à respecter et à se soumettre aux règles établies dans le présent document aux fins de leur utilisation du système de courrier électronique et de l'Internet.

DIRECTIVES

1. Le groupe Helios détient la propriété exclusive des systèmes électroniques de communication mis à la disposition des employés ainsi que de l'information qui s'y rattache et qui peut y être contenue. Un registre des sites Internet visités par chacun des employés est tenu et conservé sur une base journalière par l'équipe TI.

2. L'accès et l'utilisation du courrier électronique et/ou de l'Internet seront autorisés et concédés à tout employé dont le travail et les fonctions au sein de la compagnie justifient l'utilisation de tels outils et ressources. Toute demande d'accès et d'utilisation est traitée par le groupe TI sur une base de cas par cas et devra être autorisée par les directeurs de secteur concernés. La présente directive ne couvre pas l'installation, l'accès ou l'utilisation du courrier électronique ou de l'Internet à partir du domicile de l'employé. Aucune dépense encourue par un employé reliée à l'installation d'un accès Internet à son domicile ne sera remboursée par le groupe Helios, sauf si autrement stipulé.

3. L'utilisation du courrier électronique et de l'Internet est un outil de communication mis à la disposition des employés aux fins de leur travail.

4. Toutefois, l'utilisation à des fins personnelles du courrier électronique et de l'Internet est tolérée au même titre que l'utilisation à des fins personnelles du téléphone dans la mesure où cet usage est raisonnable et n'empêche pas la prestation normale du travail de l'employé et qu'il s'acquitte des tâches qui lui sont assignées.

5. Toute utilisation par l'employé du courrier électronique et de l'Internet à des fins personnelles ne doit pas non plus nuire au bon fonctionnement des opérations courantes de l'entreprise. L'employé a la responsabilité d'utiliser les ressources de l'entreprise de façon efficace, sans exposer le groupe Helios et ses systèmes à des ralentissements indus, des encombrements ou des interruptions de service ou à des situations qui pourraient porter atteinte à sa réputation ou aux droits des tiers.

6. Parce que le courrier électronique et l'Internet sont destinés avant tout à servir les intérêts et à exécuter un travail ou des services pour et au

Initiales _____

bénéfice du groupe Helios, l'employé doit être conscient que le groupe Helios ne peut assurer ou garantir la confidentialité ou la nature privée des communications transitant par ses systèmes. Toutefois le groupe Helios tentera, dans la mesure du possible, de respecter le droit à la vie privée de tout employé faisant un usage personnel du courrier électronique et de l'Internet, dans les limites et aux conditions indiquées à la présente directive.

7. L'employé a le devoir d'utiliser le courrier électronique ou l'Internet dans le respect de la dignité d'autrui et de manière à contribuer au maintien d'un milieu de travail qui soit exempt de discrimination et de harcèlement. Ainsi, toute utilisation du courrier électronique et de l'Internet impliquant ou relatif à des activités illégales ou illicites ou à connotation sexuelle ou pornographique, sous toutes ses formes, non conformes aux directives du groupe Helios ou contenant des messages d'intolérance, de menaces, de haine ou diffamatoires, est strictement interdite.

8. Le groupe Helios se réserve le droit, à sa discrétion, de bloquer l'accès à certains sites Internet qu'il considère non conformes ou ne respectant pas les règles de la présente directive ou qui encombre, alourdit ou ralentit de façon indue ses systèmes (ex. : sites diffusant de la musique).

9. En raison de l'encombrement du réseau et du nombre croissant d'utilisateurs et de données stockées dans ses systèmes, l'employé doit restreindre au strict minimum les fichiers de nature personnelle enregistrés sur le réseau. Tout courrier électronique personnel reçu, notamment avec un fichier joint, ne devra pas être conservé par l'employé dans le réseau et devra être supprimé après lecture.

10. De même, la transmission ou la réception de blagues par le biais du courrier électronique et de l'Internet devront être traitées au même titre qu'une communication de nature personnelle et, en conséquence, être faites en respect des règles de la présente directive. Elles ne devront pas être conservées ni enregistrées dans le réseau du groupe Helios et devront être détruites après lecture.

Initiales _____

11. Advenant que le groupe Helios constate un usage inapproprié et non conforme aux termes de la présente directive, le groupe Helios se réserve le droit, lorsque pertinent, de vérifier l'utilisation faite par tout employé du courrier électronique et de l'Internet de même que des adresses ou sites visités ou impliqués. Dans les circonstances où un employé abuserait de ce privilège, le groupe Helios prendra les mesures correctives qu'il considère appropriées à son encontre.

12. Le courrier électronique interne du groupe Helios est un système privé. Toutefois, le courrier électronique externe (via le réseau Internet) ne peut être considéré comme privé et ne protège pas la confidentialité des informations qui y sont véhiculées. Puisqu'il n'est pas illégal d'accéder aux données transmises par autrui sur Internet, l'employé doit utiliser ce mode de communication avec les précautions nécessaires et d'usage. Par exemple, un message transmis sur Internet peut être intercepté par quelqu'un de l'extérieur de l'entreprise tout autant que le propriétaire d'un site Internet visité peut facilement identifier l'origine d'une consultation.

13. Le service des technologies de l'information s'est doté d'un logiciel antivirus corporatif qu'il tient à jour. Cependant, les logiciels antivirus sont toujours un pas derrière les créateurs de virus. Il est en conséquence important de se méfier de tout ce qui est téléchargé d'Internet, tout particulièrement des fichiers attachés aux courriers électroniques. Les problèmes commencent généralement lorsque l'on «double-clique» sur ces fichiers attachés pour les ouvrir. Alors, ne jamais le faire à la légère. Le groupe Helios demande donc à ses employés d'être particulièrement vigilants. Veuillez rapporter au centre d'assistance du service des technologies de l'information tout virus constaté ou fichier suspect.

14. Tout manquement à la présente directive peut entraîner l'imposition de mesures disciplinaires pouvant aller jusqu'au congédiement.

2.11 Clé USB ou autres médias externes

Il est important de protéger toutes les informations importantes qui se trouvent sur votre clé USB. Spécifiquement l'information confidentielle. Vous pouvez le faire par le biais d'encryption. L'information sera alors inutilisable si l'équipement est volé ou perdu. Le service TI vous indiquera comment faire.

Initiales _____

2.12 Les PC et portables des personnes distantes

- Les PC n'ouvrent pas de session directe sur le réseau du groupe Helios. Ils le font par le biais d'une session locale.
- Les PC doivent être protégés par un processus de mise en session local.
- Les PC doivent être protégés par un antivirus corporatif qui détecte également les «spyware / malware».
- La mise à jour de la définition des virus et de sécurité Windows doit se faire de façon automatique.

Lors de la connexion à Internet, le coupe-feu de Windows doit être activé.

2.13 Les PC et portables

- Les portables doivent être protégés par un processus de mise en session.
- L'usager doit se mettre en session avec les serveurs Windows afin d'obtenir accès aux services informatiques.
- La personnalisation et les installations de logiciels portables doivent être réservées aux conseillers informatiques.
- Les portables doivent être protégés par un antivirus corporatif qui détecte également les «spyware / malware».
- Les portables sont mis hors session après 30 minutes.

Initiales _____

ANNEXE A

Classification de l'accessibilité de l'information

Classification	Description	Accessibilité
Publique	Est considérée publique toute information qui est du domaine public.	Sans restriction
Confidentielle	Est considérée confidentielle toute information non connue du public sur le groupe Helios, ses activités, ses employés, ses fournisseurs, ses partenaires, etc. Toute information sensible qui, si elle devait être divulguée sans autorisation, pourrait porter atteinte aux intérêts du groupe Helios (ainsi qu'à ceux de ses employés, fournisseurs ou partenaires). Les différentes catégories suivantes donnent des exemples d'informations confidentielles. Notons que les catégories et les exemples qu'elles contiennent ne constituent en aucun cas une liste exhaustive. **Renseignements personnels confidentiels** • Numéro d'assurance sociale, numéro de téléphone, numéro de compte bancaire, dossier de crédit, date de naissance, adresse postale, âge, sexe, adresse de courriel personnelle, etc. • État matrimonial, dossier médical, etc. (d'un employé). • Tout bloc d'information permettant d'identifier un individu de façon précise (employé). **Renseignements confidentiels d'un tiers confiés à l'entreprise** • Renseignements financiers, commerciaux, scientifiques, techniques ou syndicaux de nature confidentielle fournis par un tiers et habituellement traités par un tiers de façon confidentielle. **Renseignements ayant des incidences sur l'entreprise** • L'information provenant des contrats commerciaux. • L'information sur les contrats avec les partenaires et fournisseurs. • L'information concernant les stratégies d'investissements et la concurrence. • Mandat ou stratégie de négociation de convention collective. • Transaction ou projet de transaction relatif à des biens, des services ou des travaux. • Opinions juridiques. • Mémoires ou délibérations de toute instance décisionnelle. • Avis ou recommandations du personnel, d'un consultant ou d'un autre organisme.	Accessible au personnel qui a obtenu l'autorisation explicite d'y accéder

Initiales _____

	• Épreuve destinée à l'évaluation comparative des connaissances, des aptitudes ou de l'expérience d'une personne. • Renseignements obtenus par une personne qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois. • Renseignements sous le couvert d'un interdit de communication ou d'une ordonnance de non-publication, de non-divulgation ou de non-diffusion. • Renseignements sur les dispositifs de sécurité de l'entreprise. • Renseignements sur les résultats financiers anticipés de l'entreprise.	

Initiales _____

ANNEXE B

Classification de la disponibilité de l'information

Classification	Description	Accessibilité
Critique	Information dont la disponibilité est **critique** pour la mission de l'entreprise et dont la non-disponibilité n'est tolérable que pour un court délai.	48 heures
Essentielle	Information dont la disponibilité est **essentielle** aux activités de l'entreprise et dont la non-disponibilité n'est tolérable que pour un court délai.	Entre 3 et 7 jours
Non essentielle	Information dont la disponibilité est **non essentielle** aux activités de l'entreprise et dont la non-disponibilité est tolérable pour un délai prolongé.	Plus de 7 jours

Signature de l'employé	
Paraphez chaque page	Nom :
	Fonction :
	Signature :
	Date :

Initiales _____