

Titre Gestion et protection de l'information		Numéro Dir-06
		Révision <input checked="" type="checkbox"/> oui <input type="checkbox"/> non
		En vigueur le
Unités émettrices: directions principales Approvisionnement et Services, Contrôle et Comptabilité, Technologies de l'information, vice-présidence Affaires corporatives et Secrétariat général	Approbation André Caillé - original signé et conservé Président-directeur général	Date 2000/12/20
Activité(s) visée(s) Toutes les activités de l'entreprise		

1. Définition

- **Information**

Idées, savoir, connaissances, renseignements représentés par des textes, des images, des paroles, des données, des documents, fixés sur un support (papier, disquette, serveur, bande magnétique...) ou non et qui appartiennent à l'entreprise ou qui lui ont été confiés.

2. Règles à observer et mesures à prendre

- **Responsabilité du personnel et des gestionnaires**

Le personnel de l'entreprise est responsable, dans le cadre de ses fonctions, de gérer efficacement et de protéger judicieusement l'information, en fonction de sa nature, de ses caractéristiques et de sa valeur.

Les gestionnaires des unités qui produisent ou détiennent l'information sont responsables de fournir les autorisations prévues dans les présentes règles.

- **Accessibilité, utilisation et non divulgation**

Le personnel doit avoir libre accès à l'information nécessaire à son travail.

Le personnel doit accéder et utiliser l'information selon les autorisations accordées.

Le personnel ne doit jamais divulguer l'information confidentielle sans autorisation explicite.

L'entreprise doit exiger de ses partenaires et fournisseurs, dont les consultants, qu'ils s'engagent par écrit à ne pas divulguer l'information qui leur est confiée, ni à l'utiliser pour leur profit ou celui d'un tiers.

L'entreprise doit s'assurer que ses employés connaissent les règles d'utilisation et de non divulgation de l'information.

- **Information exacte, à jour et fiable**

L'information doit être exacte et maintenue à jour, aussi longtemps qu'il est nécessaire. En cas de doute, la fiabilité de l'information doit être vérifiée.

Toute modification aux systèmes d'information doit faire l'objet d'une documentation écrite.

- **Description et classification**

Titre Gestion et protection de l'information	Numéro Dir-06
--	-------------------------

L'information doit faire l'objet d'une description uniformisée dans l'entreprise pour en faciliter le repérage, la conservation et la protection.

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

- **Mesures de sécurité**

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

Des mesures de sécurité (ex.: copies partielles ou modifiées, profils d'utilisation) doivent être prises lorsque des copies de données informatiques sont requises à des fins de test ou de formation.

Des mesures de sécurité (ex.: révocation ou modification des accès) doivent être prises lorsque les employés sont mutés, qu'ils quittent l'entreprise ou lorsque les dossiers auxquels sont affectés les consultants sont terminés.

Des mesures de sécurité (ex. : détection des virus informatiques, authentification manuelle ou signature électronique, vérifications simultanées, 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, au besoin.

Des mesures de sécurité (ex. : copies, mises en voûte, 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 s'adapter au niveau de classification de l'accessibilité et de disponibilité de l'information (classifications décrites en annexe). L'accès à toute information doit être donné en fonction du besoin de savoir ou de faire et en fonction du travail demandé à l'employé (ex.: code d'utilisateur, certificat, profil d'utilisation, accès à une filière).

- **Suivi des accès accordés**

Un suivi des accès accordés (accès aux bâtiments, aux données) doit être effectué par le biais d'un registre permettant de vérifier que les accès sont justifiés et dûment autorisés.

- **Conservation et disposition**

L'information doit être conservée aussi longtemps qu'il est nécessaire, en fonction des besoins opérationnels de l'entreprise et des cadres réglementaires qui s'appliquent.

L'information qui n'a plus à être conservée doit être détruite selon les procédures établies.

Le patrimoine informationnel de l'entreprise doit être archivé et mis en valeur.

- **Propriété intellectuelle et valeur commerciale**

La propriété intellectuelle de l'entreprise doit être protégée par l'unité qui en est dépositaire en procédant aux enregistrements requis, s'il y a lieu, dont la prise de

Titre	Numéro
Gestion et protection de l'information	Dir-06

brevet. L'information qui a une valeur commerciale doit être protégée.

- **Veille informationnelle**

Les unités de l'entreprise doivent colliger efficacement l'information importante pour la réalisation de la mission de celle-ci ou de ses orientations stratégiques.

3. Mécanismes de suivi

La présente directive est émise conjointement par les unités administratives suivantes: direction principale Approvisionnement et Services, direction principale Contrôle et Comptabilité, direction principale Technologies de l'information et vice-présidence Affaires corporatives et Secrétariat général.

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:

1. Vérification régulière du respect des règles stipulées dans la directive et les encadrements qui en découlent, selon une planification qui tient compte des sujets à traiter en priorité. Des rapports seront remis aux gestionnaires responsables des unités visées.
2. 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.
3. Programmes permanents d'information et de sensibilisation à la directive et aux encadrements qui en découlent.
4. 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.

4. Liste des annexes

Annexe 1. Classification de l'accessibilité et de la disponibilité de l'information.

Gestion et protection de l'information

Classification de l'accessibilité de l'information

Classification	Description	Accessibilité
Publique	Information destinée à être diffusée publiquement, ou qui a été rendue publique par l'entreprise, dont la diffusion ne peut porter atteintes aux intérêts de l'entreprise.	Sans restriction.
Confidentielle	<p>Information sensible qui, si elle devait être divulguée sans autorisation, pourrait porter atteinte aux intérêts de l'entreprise (ainsi qu'à ceux de ses employés, clients, fournisseurs ou partenaires), du gouvernement ou d'autres organismes publics.</p> <p>⇒ <i>Renseignements personnels confidentiels</i></p> <ul style="list-style-type: none"> • Numéro d'assurance sociale, numéro de téléphone, dossier de crédit, date de naissance, adresse antérieure (d'un client) • Numéro d'assurance sociale, âge, état matrimonial, dossier médical, adresse, numéro de téléphone personnel (d'un employé) <p>Se référer au document publié par le Secrétariat général (mai 1995 et modifications) intitulé <i>Droit à l'information et respect de la vie privée</i> et à la section Affaires corporatives et gouvernementales du site Intranet de l'entreprise.</p> <p>⇒ <i>Renseignements confidentiels d'un tiers confiés à l'entreprise</i></p> <ul style="list-style-type: none"> • Secrets industriels ou renseignements industriels, financiers, commerciaux, scientifiques, techniques ou syndicaux de nature confidentielle fournis par un tiers et habituellement traités par un tiers de façon confidentielle • Renseignements industriels, financiers, commerciaux, scientifiques ou techniques lui appartenant et dont la divulgation risquerait vraisemblablement d'entraver une négociation en vue de la conclusion d'un contrat, de causer une perte à ce tiers, de procurer un avantage appréciable à une autre personne ou de nuire de façon substantielle à la compétitivité de ce tiers <p>⇒ <i>Renseignements ayant des incidences sur l'économie de l'entreprise</i></p> <ul style="list-style-type: none"> • Secrets industriels de l'entreprise • Renseignements industriels, financiers, commerciaux, scientifiques ou techniques dont la divulgation risquerait vraisemblablement d'entraver une négociation en vue de la conclusion d'un contrat, de causer une perte à l'entreprise, de nuire de façon substantielle à sa compétitivité, de procurer un avantage appréciable à une autre personne • Toute l'information concernant les clients, leur profil, leur consommation, leurs équipements • L'information provenant des recherches commerciales • L'information sur les contrats avec les partenaires et fournisseurs • L'information concernant les stratégies commerciales et la concurrence • Mandat ou stratégie de négociation de convention collective • Étude préparée en vue de l'imposition d'une taxe, d'un tarif ou d'une redevance • Transaction ou projet de transaction relatif à des biens, des services ou des travaux <p>⇒ <i>Renseignements ayant des incidences sur les décisions administratives de l'entreprise</i></p>	<p>Accessible au personnel qui a obtenu l'autorisation explicite d'y accéder.</p>

Titre Gestion et protection de l'information	Numéro
--	--------

	<ul style="list-style-type: none"> • Opinions juridiques • Version préliminaire ou tout projet de texte réglementaire • Mémoires ou délibérations d'une séance du Conseil d'administration • Avis ou recommandations du personnel, d'un consultant ou d'un autre organisme • Analyse produite à l'occasion d'une recommandation faite dans le cadre d'un processus décisionnel en cours • Analyse dont la divulgation risquerait vraisemblablement d'avoir un effet sur une procédure judiciaire • Épreuve destinée à l'évaluation comparative des connaissances, des aptitudes ou de l'expérience d'une personne <p>⇒ <i>Renseignements ayant des incidences sur l'administration de la justice et la sécurité publique</i></p> <ul style="list-style-type: none"> • 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 portant sur une méthode ou une arme susceptible d'être utilisée pour commettre un crime ou une infraction à la loi <p>⇒ <i>Renseignements ayant des incidences sur la vérification de l'entreprise</i></p> <p>⇒ <i>Renseignements qui porteraient préjudice à la conduite des relations entre le gouvernement du Québec et un autre gouvernement ou une organisation internationale</i></p> <p>⇒ <i>Renseignements qui entraveraient une négociation avec un autre organisme public</i></p>	
--	---	--

Classification de la disponibilité de l'information

Classification	Description	Disponibilité
Critique	Information dont la disponibilité est critique pour la mission de l'entreprise et dont la non-disponibilité n'est tolérable que pour un très court délai.	24h. ou moins
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 1 et 7 jours.