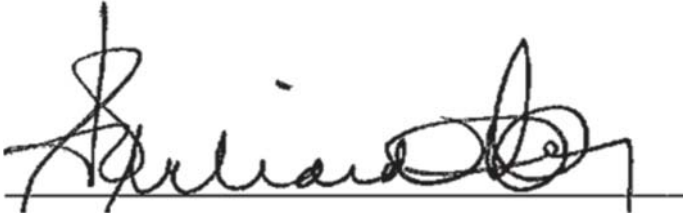


Directive

Utilisation des systèmes d'information

<p>Numéro : DAP-009</p> <p>Date d'entrée en vigueur : Date 2014-09-01</p> <p>Responsable : Jacques Martin Directeur TI</p>	<p>Diffusion : Tout le personnel</p> <p>Approuvée par : Richard Roy VP TI et Logistique</p> <div style="text-align: center;">  </div> <p style="text-align: center;">Signature</p>
---	---

Directive

Utilisation des systèmes d'information

Approbateur et collaborateurs

Approbateur	Vice-président approvisionnement et réglementation
Collaborateurs	Direction affaires juridiques et réclamations Direction soutien à la performance et relations employés Direction de l'audit interne

Historique des révisions

Version	Date	Description	Auteur
1.0	2014/09/01	Rédaction initiale avec le nouveau gabarit	Martin Vézina
2.0	2018/02/15	Changer Gaz Métro pour Énergir	Nancy Morrissette
2.1	2018/02/15	Changer Gaz Métro pour Énergir	Nancy Morrissette
2.2	2018/02/15	Changer Gaz Métro pour Énergir	Nancy Morrissette

Utilisation des systèmes d'information

Table des Matières

1. POSITIONNEMENT ET ENGAGEMENT DE L'ENTREPRISE	4
2. OBJECTIFS	4
3. CHAMP D'APPLICATION	4
4. PORTÉE	4
5. RESPONSABILITÉS DE L'UTILISATEUR	4
6. DROITS D'ENERGIR	6
7. CONTEXTES SPÉCIFIQUES	7
Endroits publics et télétravail	7
Échange d'information	7
Ordinateurs portables.....	8
Téléphones intelligents et tablettes électroniques	8
Utilisation des courriels	9
Appels téléphoniques.....	10
Médias sociaux	10
Programme d'utilisation de systèmes d'information personnel	11
8. RÉFÉRENCES	12

Utilisation des systèmes d'information

1. POSITIONNEMENT ET ENGAGEMENT DE L'ENTREPRISE

Société en commandite Énergir (« Énergir »), reconnaît que les systèmes d'information sont essentiels à ses opérations et, de ce fait, qu'ils doivent faire l'objet d'une évaluation, d'une utilisation appropriée et d'une protection adéquate.

En conséquence, tous les utilisateurs des systèmes d'information sous la responsabilité d'Énergir sont visés par les règles de la présente directive d'utilisation des systèmes d'information (la « Directive ».)

Les utilisateurs qui dérogent sans autorisation à la Directive s'exposent à des mesures disciplinaires pouvant aller jusqu'au congédiement.

2. OBJECTIFS

La Directive vise à encadrer l'usage des systèmes d'information d'Énergir et, en particulier, à prévenir toute utilisation illégale, fautive, abusive, déraisonnable ou non autorisée.

Énergir prend des mesures techniques pour protéger ses systèmes d'information et les informations qu'ils contiennent. Cependant, cette protection n'est pas absolue et l'implication des utilisateurs est indispensable pour assurer une protection optimale.

Cette directive vise donc à énoncer les règles à respecter à l'égard de l'usage et du traitement de l'information et de l'utilisation des systèmes d'information. Elle vient supporter la Politique de sécurité de l'information.

3. CHAMP D'APPLICATION

La Directive s'applique à tous les utilisateurs des systèmes d'information d'Énergir.

4. PORTÉE

La Directive s'applique à l'ensemble des systèmes d'information utilisés pour le bénéfice d'Énergir.

5. RESPONSABILITÉS DE L'UTILISATEUR

L'utilisateur est responsable de toutes les activités effectuées à partir du ou des compte(s) attribué(s) par Énergir dans le cadre de son travail et il doit respecter les règles suivantes :

1. Protéger la confidentialité des informations auxquelles il accède, qu'il transmet, modifie ou détruit. Il ne doit jamais utiliser ou révéler des informations confidentielles au détriment de l'entreprise, des membres du personnel ou pour son gain personnel.
2. Respecter ses droits d'accès et accéder uniquement aux actifs informationnels nécessaires pour remplir ses fonctions chez Énergir; le cas échéant, les droits d'accès

Utilisation des systèmes d'information

supplémentaires, temporaires ou spéciaux doivent être demandés explicitement auprès de son gestionnaire et approuvés par le propriétaire de l'actif informationnel visé. L'utilisateur est responsable d'aviser son gestionnaire s'il détient des droits d'accès plus larges que ceux requis par ses fonctions. Ces droits d'accès devront être révoqués.

3. Prendre tous les moyens raisonnables à sa disposition afin de protéger les systèmes d'information appartenant à Énergir.
 4. Ne pas tenter de contourner des contrôles mis en place par Énergir.
 5. Protéger les mots de passe qui lui sont attribués dans le cadre de son travail et ne pas permettre à une autre personne d'utiliser ses comptes personnels.
 6. Protéger les systèmes d'information portatifs qui lui sont fournis afin de prévenir les bris, les vols d'équipement et les vols de données.
 7. Se procurer les systèmes d'information utilisés dans le cadre des activités d'affaires par l'entremise du centre de service des technologies de l'information (CSTI).
 8. Communiquer avec la sûreté dans les plus brefs délais lorsqu'un système d'information est perdu ou volé.
 9. Aviser son gestionnaire ainsi que le responsable de la sécurité de l'information dans les plus brefs délais s'il est témoin ou s'il détecte une des situations suivantes pouvant porter atteinte à Énergir ou à son personnel :
 - tentative d'extorsion d'information confidentielle, telle que des mots de passe ou des documents stratégiques;
 - menace générale ou visant spécifiquement Énergir, mais ne se limitant pas à des défauts ou vulnérabilités, des programmes malveillants, des virus informatiques, une utilisation inappropriée ou malveillante des actifs informationnels d'Énergir.
 10. Effectuer périodiquement le ménage de fichiers dans ses répertoires personnels et sur le réseau d'Énergir afin de s'assurer qu'ils sont toujours nécessaires.
 11. Utiliser les systèmes d'information :
 - de façon à ne causer aucun préjudice à Énergir;
 - dans le respect de la loi et des bonnes mœurs.
 12. Ne pas effectuer les activités suivantes :
 - modifier, transformer, reconfigurer les systèmes d'information fournis par Énergir de façon à les utiliser hors de leur contexte d'affaires sans approbation par les propriétaires des systèmes; en particulier, d'utiliser une carte de transmission de
-

Utilisation des systèmes d'information

données supportée par Énergir dans un appareil qui n'est pas la propriété d'Énergir;

- utiliser sans autorisation des systèmes d'information personnel pour les activités d'affaires d'Énergir; en particulier, utiliser un ordinateur personnel branché directement sur le réseau informatique d'Énergir ou un téléphone cellulaire personnel en conjonction avec une carte SIM associée à Énergir;
- accéder ou utiliser des sites Internet inappropriés (ex : illégaux, contenu adulte, violence...). À moins d'un avis contraire de son gestionnaire, il est permis d'effectuer un usage raisonnable de l'accès Internet à des fins personnelles. Cette utilisation ne doit pas nuire à la prestation de travail de l'employé;
- consulter, télécharger, distribuer ou créer du matériel offensant, hostile, raciste, sexiste, haineux, diffamatoire, discriminatoire, pornographique ou à connotation sexuelle;
- commettre des activités illégales et/ou frauduleuses;
- contrevenir à la propriété intellectuelle, notamment, aux droits d'auteur, aux marques de commerce ou aux brevets;
- diffuser un envoi de courriels massif sans une autorisation préalable; de façon générale, tout message transmis par le réseau de courrier électronique d'Énergir doit être ciblé au(x) destinataire(s) concerné(s);

6. DROITS D'ÉNERGIR

Afin d'assurer la sécurité de ses actifs informationnels, Énergir peut notamment :

1. Bloquer l'accès à certains sites Internet jugés non pertinents aux besoins de l'entreprise.
2. Surveiller les informations accédées, transmises, entreposées, détruites ou reçues par les systèmes d'information sous sa responsabilité.
3. Filtrer et archiver le contenu de toutes les informations accédées, transmises, entreposées, détruites ou reçues par ses systèmes d'information.
4. Aviser l'utilisateur, l'expéditeur d'un courriel, les responsables des ressources humaines ou un responsable de la sécurité de l'information lors de l'utilisation jugée inappropriée de ses systèmes d'information, tel que décrit dans les énoncés précédents.

Utilisation des systèmes d'information

7. CONTEXTES SPÉCIFIQUES

Endroits publics et télétravail

L'accès à distance aux infrastructures d'Énergir dans le cadre du télétravail doit être autorisé spécifiquement par le gestionnaire de l'utilisateur.

L'utilisateur doit porter une attention particulière à la confidentialité des informations qu'il détient et/ou accède en lien avec Énergir dans les endroits publics, il doit en particulier :

1. Éviter de se connecter aux systèmes (ex : courriels et prise de contrôle du poste de travail à distance) d'Énergir en utilisant un poste de travail public (ex : lobby d'un hôtel et bibliothèque) car ces postes sont très susceptibles de contenir des logiciels malicieux qui pourraient subtiliser les codes d'accès et mots de passe. Ce type d'accès ne devrait s'effectuer qu'à partir de postes de travail de confiance (présence d'un antivirus à jour et application régulière des mises à jour logicielles).
2. Faire preuve de prudence lors de l'accès aux systèmes afin d'éviter d'exposer des renseignements confidentiels à des tiers.
3. Protéger physiquement les systèmes d'information portatifs utilisés en évitant de les laisser sans surveillance ou sans protection.

Échange d'informations

Dans la conduite des affaires d'Énergir, il arrive fréquemment que les utilisateurs doivent échanger des informations avec des tiers. De plus, on doit aussi considérer le cas d'employés qui ont besoin d'accéder à des documents du travail sur leurs équipements personnels lorsqu'ils veulent travailler de la maison. Dans ce contexte, on doit s'assurer que la mécanique des échanges permet de préserver la confidentialité des informations échangées en transport et en stockage. En particulier, on doit s'abstenir de communiquer des informations confidentielles non protégées en utilisant des services qui ne permettent pas d'assurer la confidentialité du contenu. À cet effet, les utilisateurs ne doivent pas transmettre ce type d'information sur des infrastructures non supportées par Énergir, mais ne se limitant pas au courriel personnel (ex : Hotmail, Gmail, Videotron...) ou à un service de sauvegarde de l'information sur Internet (ex : Dropbox, Skydrive...). En cas de besoin à cet effet, les utilisateurs doivent contacter la direction des technologies de l'information.

Utilisation des systèmes d'information

Ordinateurs portables

Les ordinateurs portables appartenant à Énergir doivent être :

1. fixés à un point d'ancrage solide avec un câble de verrouillage, et ce, en tout temps, excepté en transport;
2. branchés régulièrement sur le réseau informatique d'Énergir, afin que les processus de mise à jour et de synchronisation des données s'effectuent normalement.

Téléphones intelligents et tablettes électroniques

Les téléphones intelligents et tablettes électroniques appartenant à Énergir doivent être fournis et configurés par le CSTI pour s'assurer de respecter les normes d'Énergir. Les activités suivantes sont proscrites pour ces appareils :

1. brancher le téléphone à un système d'information tiers (n'appartenant pas à l'utilisateur ou Énergir), même pour le recharger;
2. transférer de l'information confidentielle à partir d'un de ces appareils vers un autre système d'information hors du contrôle d'Énergir;
3. utiliser le téléphone à titre de modem à des fins personnelles sans obtenir une autorisation préalable du CSTI;

Utilisation des systèmes d'information

Utilisation des courriels

Les courriels sont utilisés comme vecteur d'attaque dans le cadre de plusieurs menaces informatiques. Énergir met en place différents moyens de protection à cet effet, mais ils ne constituent pas de moyens de défenses infaillibles. Par conséquent, l'utilisateur doit accorder une attention particulière aux courriels non sollicités, d'origine douteuse ou inconnue. En particulier avant d'ouvrir un courriel, de cliquer sur un lien qu'il contient ou d'ouvrir un fichier attaché, l'utilisateur doit faire preuve de la plus grande prudence et, en cas de doute, il doit contacter un responsable de la sécurité de l'information; voici des exemples de questions à se poser avant d'agir :

- Est-ce que le courriel provient de l'extérieur de l'entreprise?
- Est-ce que le courriel provient d'une source ou d'une personne connue?
- Est-ce qu'on demande des informations sensibles (informations confidentielles sur l'entreprise, informations personnelles)?
- Est-ce qu'on me demande de fournir mon mot de passe, mon NIP ou d'autres informations de ce type?
- Le fichier attaché ou le lien Internet est-il utile dans le cadre des fonctions de mon travail? Est-il normal qu'il se retrouve dans ce courriel?

Il ne faut jamais relayer des courriels de publicité non sollicités ou qui demandent à être redirigés (« SPAM », « chaîne de lettres » et autres). Ils devraient être effacés sans y répondre et sans les rediriger. Dans le cas où un utilisateur reçoit un volume anormalement élevé de courriels non sollicités, il peut en informer le CSTI qui pourra alors procéder à des vérifications.

Directive

Utilisation des systèmes d'information

Appels téléphoniques

Les appels téléphoniques peuvent être utilisés comme vecteur d'attaque dans le cadre de plusieurs menaces informatiques. En utilisant des techniques d'ingénierie sociale, des individus ou groupes malveillants peuvent obtenir l'accès à des systèmes et/ou de l'information confidentielle d'Énergir. On doit donc faire preuve de vigilance. En cas de doute, il peut être utile de prendre le numéro en note, de vérifier la provenance et de rappeler ensuite. Voici des exemples de questions à se poser avant de fournir des informations au téléphone :

- Est-ce que l'appel provient de l'extérieur de l'entreprise?
- Est-ce que l'appel provient d'une source ou d'une personne connue?
- Est-ce qu'on demande des informations sensibles (informations confidentielles sur l'entreprise, informations personnelles)?
- Est-ce qu'on me demande de fournir mon mot de passe, mon NIP ou d'autres informations de ce type?
- Est-ce qu'on demande d'utiliser un site Internet ou de répondre à un courriel qui pourrait avoir des impacts négatifs sur l'entreprise ou sur mon travail?

Médias sociaux

Le secteur stratégie, communication et développement durable est responsable d'encadrer l'utilisation des médias sociaux à Énergir. Les employés doivent se référer au Guide d'utilisation des médias sociaux pour y connaître les conditions d'utilisation.

Utilisation des systèmes d'information

Programme d'utilisation de systèmes d'informations personnels

Énergir a en place un programme où des employés peuvent utiliser leur téléphone et/ou tablette personnelle pour avoir accès à certaines ressources liées à leur emploi. Un employé qui décide de participer à ce programme doit se conformer à certaines règles de base dont l'objectif est d'assurer la protection des informations d'Énergir :

- L'employé est responsable d'appliquer régulièrement les mises à jour et mises à niveau proposées par le fournisseur ou le fabricant du système;
- L'employé ne doit jamais déverrouiller le système (« *jailbreak* »);
- L'employé est responsable d'aviser le CSTI en cas de perte ou vol de son système d'information personnel;
- L'employé doit se soumettre à des mesures de sécurité obligatoires telles que les règles de complexité pour les mots de passe ainsi que le verrouillage automatique de l'appareil suite à une période d'inactivité.

La participation à ce programme est un privilège et l'autorisation d'utiliser un système d'information personnel intégré à Énergir et les droits d'accès qui y sont associés peuvent être révoqués en tout temps, sans préavis :

- Énergir demeure propriétaire des actifs informationnels mis à la disposition des utilisateurs, il peut en disposer selon ses besoins et, en particulier, les effacer du système d'information personnel s'il le juge nécessaire;
 - Advenant la résiliation de la présente entente, notamment en cas de cessation d'emploi, l'utilisateur autorise Énergir à procéder à la destruction de l'espace de travail virtuel d'Énergir présent sur le système d'information personnel;
 - l'utilisateur est considéré comme étant propriétaire du système, ainsi que des équipements et logiciels fournis avec le système; il ne peut céder ce droit sans en aviser Énergir au préalable;
 - l'utilisateur est responsable du soutien technique de son système d'information personnel, à moins d'exclusions explicitement stipulées par Énergir;
 - aucun frais ou allocation afférent à l'utilisation du système ne sera payé ou remboursé par Énergir;
 - aucun frais ne sera facturé à l'utilisateur pour l'utilisation de son système personnel sur le réseau ou les infrastructures d'Énergir (par exemple, frais de synchronisation aux systèmes d'information d'Énergir ou autres frais).
-

Utilisation des systèmes d'information

L'utilisateur accepte qu'Énergir procède à des audits périodiques afin de s'assurer qu'elle respecte les mesures de sécurité énoncées dans la présente directive. Dans le cadre de ces vérifications, Énergir ne pourra jamais avoir accès aux informations personnelles de l'utilisateur. L'utilisateur peut décider à tout moment de cesser sa participation à ce programme.

8. RÉFÉRENCES

Politique – Sécurité de l'information

Ce document est disponible dans la section Politiques-Directives de l'intranet.

Glossaire du cadre normatif d'Énergir

Ce document est disponible dans la section Politiques-Directives de l'intranet.

DRH 13 – Informations confidentielles

Ce document est disponible dans la section Politiques-Directives de l'intranet.

Directive – Protection des renseignements personnels

Ce document est disponible dans la section Politiques-Directives de l'intranet.