La sécurité de l'information

Protéger pour mieux sauvegarder

1er juin 2017

Diane Durand et Julie Guilbeault

Hydro Québec

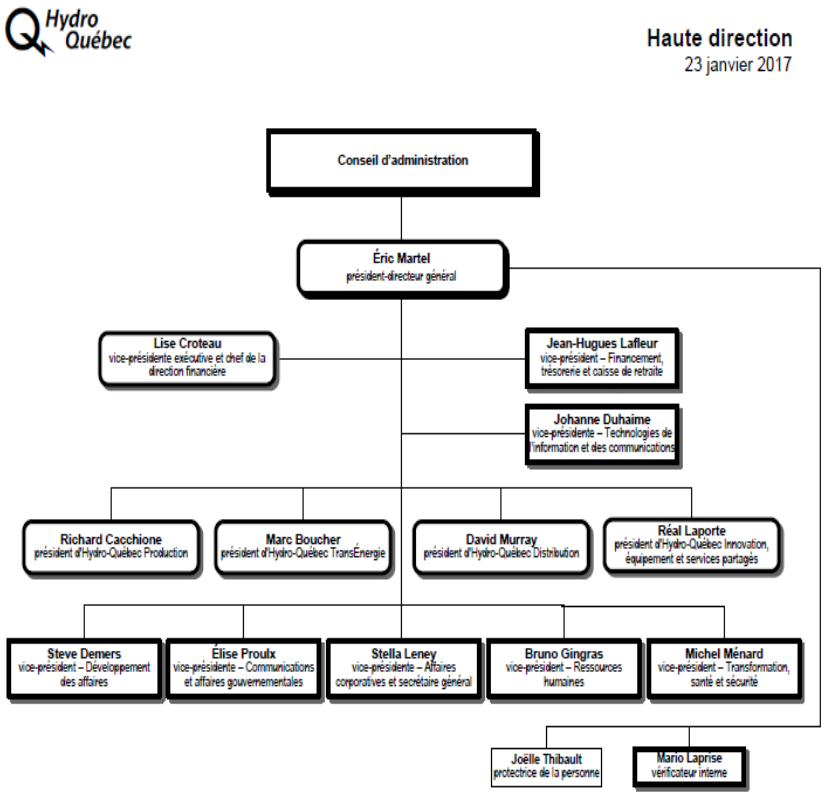
Plan de la présentation

- Portrait d'Hydro-Québec
- Portrait de l'environnement réglementaire
- Portrait de la gestion documentaire
- Portrait de la sécurité
- L'origine de la sécurité informationnelle
- Le Guide d'étiquetage et de gestion sécuritaire de l'information
- La mise en œuvre à HQIESP/SEBJ
- Période de questions

Portait d'Hydro-Québec

Hydro-Québec c'est :

- 19 500 employés
- 1 conseil d'administration
- 4 divisions
  - le constructeur (HQIESP/SEBJ)
  - le producteur (HQP)
  - le transporteur (HQT)
  - le distributeur (HQD)
- 8 vice-présidences
- la protectrice de la personne
- le vérificateur interne



Portrait de l'environnement réglementaire

En tant qu'organisme public, Hydro-Québec est soumise, entre autres, à :

- la *Loi sur les archives*
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*
- la *Loi concernant le cadre juridique des technologies de l'information*
- la directive 06 – *Gestion des documents*
- la norme – *La gestion responsable des documents à Hydro-Québec*.

Portrait de l'environnement réglementaire

Deux organismes externes influencent la sécurité de l'information:

Gouvernement du Canada / Government of Canada

Commission canadienne de sûreté nucléaire

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Portrait de la gestion documentaire

La gestion documentaire de l'entreprise c'est :

- une gouvernance d'entreprise
- des équipes de GD dans chaque division ou vice-présidence
- le centre de documents semi-actifs (87 000 boîtes)
- le service des archives (17 000 boîtes)
- les centres de documentation (9)

Portrait de la sécurité

La politique interne *Nos actifs* demande au personnel de « … gérer efficacement et de façon sécuritaire ses ressources informationnelles ».

Hydro-Québec. 2013. *Politique Nos* actifs. P. 2.

Portrait de la sécurité

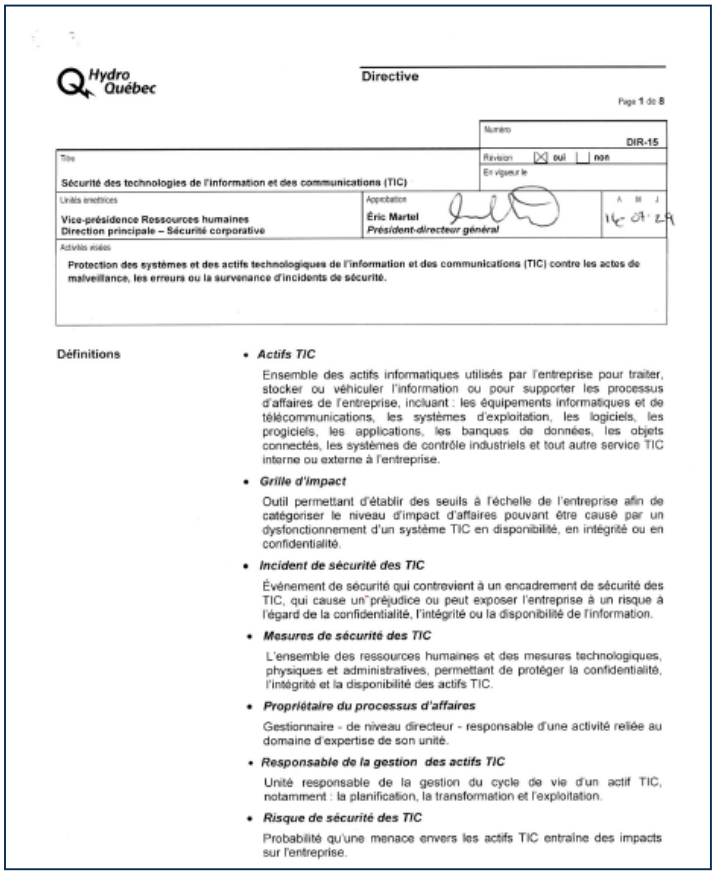
L’entreprise, par l’intermédiaire de la gouvernance en sécurité, prévoit :

- de promouvoir une culture de sécurité par l’adoption de comportements sécuritaires au sein de l'entreprise
- d’anticiper, évaluer et atténuer le risque et la menace, en étroite collaboration avec les organisations et partenaires internes et externes
- de mettre en place et maintenir des mesures de sécurité adaptées et conformes aux meilleures pratiques.

Portrait de la sécurité

- « Protection des systèmes et des actifs technologiques de l'information et des communications contre les actes de malveillance, les erreurs ou la survenance d'incidents de sécurité. »

- Hydro-Québec. 2016. *Directive 15 : sécurité des technologies de l'information et des communications* (TIC). P. 1.



Hydro Québec

Directive

Page 1 de 8

Numéro: DIR-15

Révision: ☒ oui ☐ non

En vigueur le

Titre: Sécurité des technologies de l'information et des communications (TIC)

Unités émettrices: Vice-présidence Ressources humaines, Direction principale – Sécurité corporative

Approbation: Éric Martel, *Président-directeur général*

A M J: 16 01 29

Activités visées: Protection des systèmes et des actifs technologiques de l'information et des communications (TIC) contre les actes de malveillance, les erreurs ou la survenance d'incidents de sécurité.

Définitions

- ***Actifs TIC***
  Ensemble des actifs informatiques utilisés par l'entreprise pour traiter, stocker ou véhiculer l'information ou pour supporter les processus d'affaires de l'entreprise, incluant : les équipements informatiques et de télécommunications, les systèmes d'exploitation, les logiciels, les progiciels, les applications, les banques de données, les objets connectés, les systèmes de contrôle industriels et tout autre service TIC interne ou externe à l'entreprise.
- ***Grille d'impact***
  Outil permettant d'établir des seuils à l'échelle de l'entreprise afin de catégoriser le niveau d'impact d'affaires pouvant être causé par un dysfonctionnement d'un système TIC en disponibilité, en intégrité ou en confidentialité.
- ***Incident de sécurité des TIC***
  Événement de sécurité qui contrevient à un encadrement de sécurité des TIC, qui cause un préjudice ou peut exposer l'entreprise à un risque à l'égard de la confidentialité, l'intégrité ou la disponibilité de l'information.
- ***Mesures de sécurité des TIC***
  L'ensemble des ressources humaines et des mesures technologiques, physiques et administratives, permettant de protéger la confidentialité, l'intégrité et la disponibilité des actifs TIC.
- ***Propriétaire du processus d'affaires***
  Gestionnaire - de niveau directeur - responsable d'une activité reliée au domaine d'expertise de son unité.
- ***Responsable de la gestion des actifs TIC***
  Unité responsable de la gestion du cycle de vie d'un actif TIC, notamment : la planification, la transformation et l'exploitation.
- ***Risque de sécurité des TIC***
  Probabilité qu'une menace envers les actifs TIC entraîne des impacts sur l'entreprise.

Portrait de la sécurité

Les mesures de sécurité prescrites par la directive 15 sont, entre autres :

- le respect des exigences contractuelles, législatives et réglementaires
- la classification des actifs TIC
- la détermination des besoins de sécurité TIC
- la gestion des identités et des accès
- la surveillance et la journalisation des événements de sécurité TIC

Portrait de la sécurité

En 2006 :

- Sécurité physique
- Sécurité informationnelle

En 2015 :

- Unification de la sécurité physique et informationnelle

L'origine de la sécurité informationnelle

Notre code de conduite mentionne que :

- « l'information est une ressource précieuse que nous devons protéger et gérer au même titre que les autres biens d'Hydro-Québec. »
- recommande « d'indiquer clairement le caractère confidentiel d'un document. »

Hydro-Québec. 2012. *Code de conduite : l'éthique au cœur de nos décisions*. P. 17-19.

L'origine de la sécurité informationnelle

Première version du Guide réalisée en 2009 par sécurité industrielle, sécurité des TI et gestion documentaire :

- inventorier et classifier les systèmes TIC
- respecter les exigences contractuelles, législatives et réglementaires
- un outil de bonnes pratiques basé sur :
  - la norme ISO/CEI 27001 Système de gestion de la sécurité de l'information
  - les exigences de la NERC

Deux révisions ont eu lieu en 2011 et 2015

Le Guide d'étiquetage et de gestion sécuritaire de l'information

Le Guide a été élaboré afin de :

- répondre aux exigences de sécurité de l'information
- réduire les risques liés à la divulgation non-autorisée de ladite information
- présenter les bonnes pratiques afin que tous les employés, contractuels et fournisseurs d'Hydro-Québec adaptent leurs comportements en fonction de l'étiquetage des documents

Le Guide d'étiquetage et de gestion sécuritaire de l'information

Les niveaux de confidentialité :

Niveau de confidentialité	Description
Public	Information d'ordre public.
Interne	Information disponible uniquement aux employés d'Hydro-Québec.
Confidentiel	Information dont l'accès est limité à un groupe spécifique d'employés d'Hydro-Québec et dont la divulgation accidentelle ou voulue pourrait porter préjudice à l'une des parties concernées.
Secret	Information dont l'accès est limité à un nombre restreint d'employés d'Hydro-Québec et dont la divulgation accidentelle ou voulue pourrait porter un préjudice important à l'une des parties concernées.
Très secret	Information dont l'accès est limité à un nombre très restreint d'employés d'Hydro-Québec et dont la divulgation accidentelle ou voulue pourrait porter un préjudice majeur à l'une des parties concernées.

Confidentiel (NERC)

Secret (LSRN)

Le Guide d'étiquetage et de gestion sécuritaire de l'information

La méthode d'étiquetage

Type de support	Méthode d'étiquetage préconisée
Document numérique	Identifier le niveau de confidentialité à droite dans le haut de toutes les pages. Lorsque le document est imprimé, le niveau de confidentialité doit être visible sur chacune des pages du document en incluant la page titre.
Document papier	Identifier le niveau de confidentialité à droite dans le haut de toutes les pages incluant la page titre.
Support numérique amovible (DVD, CD)	Inscrire le niveau de confidentialité le plus élevé de tous les documents à l'aide d'un marqueur à encre permanente.
Support numérique amovible réinscriptible (disque dur, clé USB)	L'étiquetage est facultatif pour ces types de supports. Au besoin, utiliser la même méthode que pour les autres supports amovibles.
Courrier électronique	Identifier le niveau de confidentialité dans l'objet (titre), uniquement pour les niveaux de confidentialité confidentiel, secret et très secret.

Le Guide d'étiquetage et de gestion sécuritaire de l'information

La méthode d'étiquetage

NERC

- Identifier sur chaque page avec la mention « Confidentiel (NERC) »

LSRN

- Identifier sur chaque page avec la mention « Secret (LSRN) »
- Contenir l'avertissement suivant en pied de page :

  « Ce document est assujetti aux dispositions de l'article 23 du *Règlement général sur la sûreté et la réglementation nucléaires*. On doit en prévenir le transfert ou la communication non autorisée par la Loi et ses règlements ».

Le Guide d'étiquetage et de gestion sécuritaire de l'information

La méthode d'étiquetage

Secret ou Très secret

- Identifier le destinataire de chaque copie produite d'un document ainsi étiqueté
  - dans le pied de page le nom du destinataire et son CII (Excel)
  - filigrane gris pâle à bordure noire où apparaissent le nom et le CII du destinataire de la copie (Word et PowerPoint)

Le guide d'étiquetage et de gestion sécuritaire de l'information

Les outils/astuces d'étiquetage :

- La macro dans la suite Office
- L'en-tête dans Adobe Acrobat
- L'estampe pour les documents papier

- Démonstration

Le Guide d'étiquetage et la gestion sécuritaire de l'information

Cet outil explique comment :

- indiquer le niveau de confidentialité
- appliquer les mesures de sécurité lors de :
  - l'entreposage du document
  - la transmission et au transport du document
  - l'impression ou la numérisation du document
  - la destruction du document

Le Guide d'étiquetage et de gestion sécuritaire de l'information

Public	Interne	Confidentiel	Secret	Mesures de sécurité
•	•	•	•	Le document doit être étiqueté
			•	Le document doit porter l'identification du destinataire : nom et CII à chaque page
				Entreposage : Support papier
•	•			Aucune mesure spéciale requise
		•		Le document doit être entreposé dans un classeur sous clé, ou dans un local à accès contrôlé
			•	Le document doit être entreposé dans un classeur sous clé et dans un local à accès contrôlé
				Entreposage : Support numérique fixe
•	•			Aucune mesure spéciale requise
		•		Le document doit être chiffré s'il y a absence de contrôle physique
			•	Le document doit être chiffré ; l'accès logique et physique au support contrôlés
				Entreposage temporaire : Support numérique amovible
•	•			Aucune mesure spéciale requise
		•	•	Le document doit être chiffré et entreposé sur un support numérique amovible appartenant à Hydro-Québec
			•	Le support amovible doit être entreposé dans un classeur sous clé de type sécurisé

Le Guide d'étiquetage et de gestion sécuritaire de l'information

Public	Interne	Confidentiel	Secret	Mesures de sécurité
				Transmission - Support papier et numérique - Intra-muros
•	•			Aucune mesure spéciale requise
		•	•	Le support doit être mis dans un contenant permettant de le dissimuler, tel une chemise ou une mallette
			•	L'information numérique doit être chiffrée
			•	Le contenant dissimulant un support papier doit être scellé et remis de main à main entre personnes autorisées
				Transmission - Support papier et numérique – Extra-muros
•				Aucune mesure spéciale requise
	•	•	•	Le support doit être mis dans un contenant permettant de le dissimuler, tel une chemise ou une mallette
		•	•	L'information numérique doit être chiffrée
		•	•	Le contenant dissimulant un support papier doit être scellé
			•	Une autorisation de transport du gestionnaire responsable de l'information est requise
			•	Un transporteur accrédité avec accusé réception doit être utilisé ou remis de main à main entre personnes autorisées
				Transmission d'information numérique - Réseaux IP, FTP, courrier électronique - Intra-muros
•	•	•		Aucune mesure spéciale requise
			•	La transmission ou l'information doit être chiffrée, exemple : Logesdes, MCT, HydroDoc
				Transmission d'information numérique - Réseaux IP, FTP, courrier électronique - Extra-muros
•	•			Aucune mesure spéciale requise
		•	•	La transmission ou l'information doit être chiffrée, exemple : Logesdes, MCT, HydroDoc

Le Guide d'étiquetage et de gestion sécuritaire de l'information

Public	Interne	Confidentiel	Secret	Mesures de sécurité
				Imprimantes (incluant numériseur et photocopieur)
•	•			Aucune mesure spéciale requise
		•	•	Une imprimante localisée dans un édifice/site d'Hydro-Québec dont l'accès est contrôlé doit être utilisée
			•	L'imprimante doit être surveillée durant l'impression
				Destruction d'un document papier
•	•			Déposer le document papier dans un bac de recyclage standard
		•	•	Déposer le document dans le bac sécurisé ou déchiqueter
				Destruction d'un support numérique (Disque dur, clé USB, DVD, CD, etc.)
•	•	•		Supprimer l'information ou détruire le support, ou disposer du support dans le bac sécurisé
			•	Contacter votre exploitant TI

La mise en œuvre à HQIESP / SEBJ

Équipement / Société d'énergie de la Baie James

- Concevoir et mettre en œuvre des projets de réfection et de construction d'équipements de production et de transport d'électricité qui répondent de façon optimale aux besoins d'Hydro-Québec. En favorisant le partenariat avec les milieux d'accueil et l'industrie, proposer des solutions performantes, rentables et alignées sur les meilleures pratiques en matière d'acceptabilité sociale et environnementale.

La mise en œuvre à HQIESP / SEBJ

Services partagés et Approvisionnement stratégique

- Fournir à l'ensemble d'Hydro-Québec les encadrements, produits et services en matière d'acquisition en adoptant les meilleures pratiques d'approvisionnement stratégiques.
- Offrir des services de gestion immobilière, de gestion de matériel, de transport et d'autres services spécialisés, de façon à contribuer à la bonne performance de l'entreprise.

La mise en œuvre à HQIESP/SEBJ

Institut de recherche

- Par la recherche et le développement, assurer le leadership de l'entreprise dans l'évolution de la connaissance et des solutions technologiques sur les éléments critiques à court et long terme pour l'amélioration de la performance de l'entreprise, en tirant le meilleur profit des produits et services présents et émergents sur les marchés.

La mise en œuvre à HQIESP/SEBJ

Implantation obligatoire à la demande du président de la division, monsieur Réal Laporte

- Axe Équipement (avril à décembre 2016)
- Axe CSP/DPAS (septembre 2016 à juin 2017)
- Axe IREQ (février à septembre 2017)

La mise en œuvre à HQIESP/SEBJ

Un travail collaboratif :

- l'unité gestion documentaire
- direction principale – Sécurité corporative
- les unités administratives

La mise en œuvre à HQIESP/SEBJ

Les critères pour déterminer les niveaux de confidentialité :

- La Loi sur l'accès
- Les exigences de la NERC et de la LSRN
- Les critères de la directive 06 – *Gestion des documents*
- Annexe A du *Guide d'étiquetage et de gestion sécuritaire de l'information* (liste d'exemples)
- Les résultats de l'analyse MEHARI (méthode harmonisée d'analyses de risques)

La mise en œuvre à HQIESP/SEBJ

Les niveaux de confidentialité établis :

- **Public** est un document déposé systématiquement sur le site Internet de l'entreprise

- **Interne** est un document qui est confidentiel au sens de la Loi

La mise en œuvre à HQIESP/SEBJ

- **Confidentiel** est un document qui comporte des renseignements :
  - personnels ou nominatifs ;
  - monétaires ou financiers ;
  - aux affaires juridiques ;
  - à la sécurisation des installations ;
  - aux stratégies d'affaires et à la gestion de risques ;
  - risquant de provoquer la perte d'avantages concurrentiels et économiques ;
  - relatifs aux respect des engagements hors recherche et développement ;
  - relatifs aux périodes préalables aux prises de brevets ou à la mise en valeur commerciale.

La mise en œuvre à HQIESP/SEBJ

- **Secret** : visé par la *Loi sur la sûreté et la réglementation nucléaire*

- **Très secret** : aucun dans la division

La mise en œuvre à HQIESP/SEBJ

L'application des niveaux de confidentialité :

- Déterminer l'étiquette appropriée à chacun des types des documents
- Validation de ces étiquettes par les représentants des directions

La mise en œuvre à HQIESP/SEBJ

Les mesures de sécurité :

- Rencontres avec la direction principale – Sécurité corporative afin de bien comprendre et de redéfinir les mesures qui portaient à confusion

- Approbation par la gestion et la haute direction de la division

La mise en œuvre à HQIESP/SEBJ

Déploiement aux employés d'Hydro-Québec :

- Élaboration de nos propres outils de formation
  - deux aide-mémoire : un pour les documents administratifs et l'autre pour les documents de mission
  - une présentation pour une formation en salle
  - une capsule vidéo de formation
- Établissement d'un calendrier d'implantation par unité. Les unités sont chargées de convoquer les réunions.

À ce jour, nous avons offert la formation

à plus de **2500 employés**

La mise en œuvre à HQIESP/SEBJ

Déploiement aux partenaires externes :

- Petites, moyennes et grandes entreprises québécoises, canadiennes et internationales
  - firmes d'ingénierie
  - entrepreneurs
  - entreprises d'achats de biens et services, etc.
- Gouvernements fédéral, provinciaux, municipaux et autochtones

La mise en œuvre à HQIESP/SEBJ

- La gouvernance d'entreprise en gestion documentaire a donc mis en place un comité spécial afin de travailler :
  - à une recommandation pour rendre l'étiquetage obligatoire dans l'entreprise
  - mettre à profit notre expérience

Conclusion

Assurer une gestion sécurisée de l'information c'est…

- Assurer la sécurité de l'information tout au long de son cycle de vie
- Sauvegarder l'expertise et le patrimoine informationnel
- Construire une culture d'entreprise dans laquelle la sécurité de l'information est une priorité

Incroyable mais vrai

- Pas de déchiquetage mais un ours qui aime le miel
- Le feu de camp avec essence et «*pépine*»
- Un sceau de cire comme au moyen-âge ou valise avec menottes
- Baisser le niveau de confidentialité pour ne pas adopter le comportement
- Torture pour les documents secrets

Période de questions


Hydro
Québec