Pour information : dirigeantreseauinformation@msss.gouv.qc.ca

RÈGLE PARTICULIÈRE SUR LA SÉCURITÉ LOGIQUE

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (L.R.Q., c. G-1.03, a. 10)
Loi sur le ministère de la Santé et des Services sociaux (L.R.Q., c. M-19.2, a. 5.2)
Loi concernant le partage de certains renseignements de santé (L.R.Q., c. P-9.0001, a. 4 et 5)

PRÉAMBULE

La présente règle particulière est définie par le dirigeant réseau de l'information (DRI) du secteur de la santé et des services sociaux dans le cadre de la mise en œuvre de la Loi concernant le partage de certains renseignements de santé (LPCRS).

SECTION I

CHAMP D'APPLICATION

1. Cette règle particulière s'applique :

   1° à un gestionnaire opérationnel d'une banque de renseignements de santé d'un domaine clinique;

   2° à un gestionnaire opérationnel du registre d'un domaine clinique;

   3° au gestionnaire opérationnel du registre des refus;

   4° au gestionnaire opérationnel du système de gestion des ordonnances électroniques de médicaments;

   5° au gestionnaire opérationnel du registre des organismes;

   6° à une personne ou une société qui héberge, opère ou exploite un actif informationnel visé par la LPCRS;

   7° à la Régie de l'assurance maladie du Québec;

   8° à un établissement visé par la Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2);

9° à une agence de la santé et des services sociaux visée par la Loi sur les services de santé et les services sociaux;

10° au Conseil cri de la santé et des services sociaux de la Baie James institué en vertu de la Loi sur les services de santé et les services sociaux pour les autochtones cris (L.R.Q., c. S-5).

Les personnes ou sociétés mentionnées à cet article sont assujetties à la présente règle particulière à l'égard des actifs informationnels auxquels s'applique la LPCRS.

SECTION II

DÉFINITIONS

2. Dans la présente règle particulière, on entend par :

1° actif informationnel : un actif informationnel au sens de la LPCRS soit une banque d'information, un système d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé;

2° authentifiant : une information confidentielle détenue par une personne et permettant son authentification;

3° autorisation d'accès minimum : une autorisation d'accès restreinte de manière à ce que l'utilisateur puisse n'accomplir avec celle-ci que les seules tâches autorisées et nécessaires à l'exercice de ses fonctions;

4° domaine de confiance : un ensemble d'éléments d'ordre juridique, humain, organisationnel et technologique, un cadre de gestion de la sécurité ou un ensemble d'activités pertinentes à la sécurité qui sont tous assujettis à une politique de sécurité administrée par une seule autorité;

5° identifiant : une information associée à une personne, connue de celle-ci ou contenue sur un support informatique dont elle est la détentrice, et qui permet son identification;

6° mécanisme : fonction de protection particulière, logicielle ou matérielle, mise en vigueur dans le cadre d'une politique de sécurité informatique;

7° périmètre de sécurité : une frontière logique délimitant l'étendue d'un domaine de confiance ou d'une zone de sécurité;

8° zone de sécurité : zone composée de segments du réseau qui partagent les mêmes conventions et règles de sécurité en termes d'accès et de niveau de confidentialité des données stockées ou traitées.

SECTION III

DOMAINE DE CONFIANCE

3. Toute personne ou société visée à l'article 1 doit mettre en place au moins un domaine de confiance ainsi que son architecture de sécurité de l'information.

4. Un domaine de confiance doit être segmenté en plusieurs zones de sécurité possédant les mesures de sécurité adaptées aux actifs informationnels hébergés dans chacune de ces zones.

5. Les environnements technologiques de production, préproduction, acceptation ou essais doivent être séparés les uns des autres par des mécanismes appropriés.

6. Un périmètre de sécurité doit être conçu et géré de manière à :

   1° contrôler les accès provenant de l'externe du domaine de confiance;

   2° contrôler les accès de l'interne du domaine de confiance vers l'externe;

   3° contrôler les communications entrantes et sortantes des actifs informationnels;

   4° surveiller les journaux associés aux mécanismes en place;

   5° évaluer régulièrement l'efficacité des mécanismes en place.

7. Toute personne ou société visée à l'article 1 qui désire publier des services, notamment sur Internet, doit évaluer les risques et mettre en place les mécanismes appropriés permettant de limiter ceux-ci.

8. La sécurité dans les échanges d'information à l'aide des télécommunications doit être assurée, notamment pour toutes communications qui vont au-delà d'un domaine de confiance.

9. Toute personne ou société visée à l'article 1 doit mettre en œuvre des mesures visant à faire en sorte que les incidents ayant trait à la sécurité logique soient déclarés au DRI conformément à la Règle particulière sur l'obligation de déclaration d'un incident de sécurité et à ce que des mesures correctrices à court et à long terme soient adoptées en temps opportun.

SECTION IV

CONTRÔLE DES ACCÈS LOGIQUES

10. Toute personne ou société visée à l'article 1 doit :

    1° appliquer le principe de l'autorisation d'accès minimum lors de l'attribution des autorisations d'accès aux actifs informationnels et ses composantes technologiques;

    2° établir une politique basée sur les meilleures pratiques de l'industrie concernant la durée des sessions des accès aux actifs informationnels;

    3° s'assurer qu'aucun renseignement de santé n'est conservé en dehors des banques de renseignements et de leurs services de gestion associés et mettre en place les processus, mécanismes et outils permettant de protéger ces renseignements durant le traitement de l'information;

    4° établir une politique basée sur les meilleures pratiques de l'industrie concernant le cycle de vie de la gestion des identifiants et des authentifiants;

    5° mettre en place un processus permettant de s'assurer de la révision des accès sur une base annuelle.

SECTION V

SURVEILLANCE ET EXPLOITATION DES INFRASTRUCTURES TECHNOLOGIQUES

11. Toute personne ou société visée à l'article 1 doit mettre en place les processus, mécanismes, outils et ressources permettant de démontrer qu'elle effectue l'exploitation de ses infrastructures technologiques de façon sécuritaire.

12. Les processus, mécanismes et outils doivent permettre de :

    1° protéger les infrastructures contre les logiciels malveillants;

    2° empêcher l'accès à des renseignements de santé à toute personne n'étant pas habilitée à en prendre connaissance;

    3° tenir à jour un registre des actifs informationnels, des composantes technologiques ainsi que leurs configurations;

    4° assurer la prise de copie des données ainsi que la récupération de ces données, le cas échéant;

5° assurer le traitement sécuritaire dans la manipulation des supports informatiques;

6° surveiller ses infrastructures et détecter les activités suspectes;

7° gérer les incidents de sécurité de l'information en respectant notamment la Règle particulière sur l'obligation de déclaration d'un incident de sécurité;

8° effectuer des analyses de vulnérabilité et des audits de sécurité;

9° assurer la mise en place des correctifs de sécurité requis concernant les actifs informationnels et leurs composantes technologiques.

13. Toute personne ou société visée à l'article 1 doit mettre en œuvre les meilleures pratiques de l'industrie concernant la journalisation logique des actifs informationnels et :

1° identifier les éléments qui doivent être contenus dans les journaux;

2° journaliser l'authentification aux actifs informationnels et ses composantes technologiques avec les éléments suivants : la date et l'heure de l'authentification, le nom de l'identifiant utilisé, et le message de confirmation de la réussite ou de l'échec de l'authentification;

3° protéger les journaux administrateurs et d'opérations contre les modifications non autorisées;

4° favoriser la séparation des tâches de vérification des journaux par une ressource distincte des administrateurs des actifs informationnels;

5° synchroniser les actifs informationnels à l'une des sources de référence indiquées à la Règle particulière sur la journalisation;

6° conserver les journaux logiques des actifs informationnels et des composantes technologiques pour une période d'un an.

SECTION VI

CONTINUITÉ DES ACTIVITÉS

14. Toute personne ou société visée à l'article 1 doit prévoir un plan de continuité des activités permettant de réduire les risques possibles de perte de service et, si nécessaire, de favoriser une reprise des activités dans les plus brefs délais. Le plan de continuité des activités doit être adapté selon la catégorisation des actifs informationnels, les impacts sur le continuum des soins et, le cas échéant, les ententes de gestion opérationnelle.

15. Le déclenchement des opérations de continuité des activités lors d'une situation de crise est considéré comme un incident de sécurité. La personne ou société visée à l'article 1 doit alors mettre en œuvre le processus de gestion des incidents de sécurité tel que spécifié à la Règle particulière sur l'obligation de déclaration d'un incident de sécurité.

SECTION VII

SÉCURITÉ APPLICATIVE

16. Toute personne ou société visée à l'article 1 doit mettre en place les processus, mécanismes, outils et ressources permettant d'assurer la sécurité :

    1° dans les actifs informationnels durant tout leur cycle de vie;

    2° dans le développement d'application, notamment la mise en place d'un cadre normatif traitant des pratiques sécuritaires de développement et assurant la prise en charge des exigences de sécurité lors du développement ou de l'acquisition de solutions technologiques.

SECTION VIII

REDDITION DE COMPTES

17. Toute personne ou société visée à l'article 1 doit transmettre au DRI, sur demande, une mise à jour de ses analyses de risques associés à la sécurité logique.

SECTION IX

DISPOSITIONS FINALES

18. La présente règle particulière a été approuvée par le Conseil du trésor le 21 mai 2013 (C.T. 212626).

19. La présente règle particulière entre en vigueur le 20 juin 2013.