Ontario Health

Norme sur la sécurité matérielle

Version: 1.8

N° de document : 3545

Gestion du document

Fréquence de révision : Une fois par année ou selon la règle établie par le Comité ConnexionSécurité.

Historique des approbations

APPROBATEURS	DATE D'APPROBATION
Connecting Security Committee	2014-11-05
Connecting Security Committee	2018-03-26
Connecting Security Committee	2021-03-18

Historique des révisions

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
1.0	2013-12-23	Adoption de la version de novembre 2013 du groupe de travail sur la protection de la vie privée et la sécurité de ConnexionRGT.	Mark Carter
1.1	2014-10-09	Révision en fonction des commentaires reçus de responsables des programmes ConnexionRGT et Connexion Sud-Ouest de l'Ontario et du groupe de protection des renseignements personnels sur la santé. Harmonisation des sections de la portée, des dérogations et de l'application avec les politiques du Comité ConnexionConfidentialité. Ajout d'une définition de « terminal d'envoi de données » et de « service de gestion d'identité ». Modification des exigences des DRS concernant les pannes au point 1.5, « devraient » devenant « doivent ». Clarification des exigences par l'ajout de mentions sur les services de gestion d'identité et les terminaux d'envoi de données un peu partout dans la section des exigences des DRS.	Mark Carter
1.2	2014-11-05	Approbation de la politique à la réunion du 5 novembre 2014 du Comité ConnexionSécurité.	Mark Carter
1.3	2015-01-21	Harmonisation du nom de la politique sur le contrôle de l'accès en fonction de la décision définitive du Comité ConnexionSécurité à l'issue de la troisième étape du processus de rédaction.	Mark Carter
1.4	2015-10-19	Mise à jour des politiques pour refléter le changement de gouvernance. Le Comité directeur a été remplacé par l'organisme de surveillance compétent. Le Comité régional de protection de la vie privée et de sécurité ne participe plus au	Mark Carter

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
		processus de décision en matière de dérogation.	
1.5	2017-03-20	Mise à jour de la norme afin de refléter l'ITSM. Changement du titre du document, qui passe de « Politique » à « Norme ». Mise à jour de la définition de « la solution de DSE ». Révision des contrôles en fonction des commentaires.	Raviteja Addepalli
1.6	2018-03-16	Mise à jour de la norme afin d'inclure l'accès au DSE par les patients.	Geovanny Diaz
1.8	2021-01-04	Examen du document avec des modifications mineures et mise à jour du cycle de révision tous les deux ans	Paul Cnudde

Norme sur la sécurité matérielle

Objet

La présente norme a pour but de définir les exigences de sécurité matérielle de [la solution de DSE] ainsi que des services de gestion d'identité et des terminaux d'envoi de données des dépositaires de renseignements sur la santé (DRS).

Portée

La présente norme s'applique à [la solution de DSE] et à l'équipe qui en est responsable, y compris la totalité des portails et des applications pour les patients.

Elle vise les éléments suivants dans le cas des DRS qui utilisent [la solution de DSE] pour voir, traiter ou autrement manipuler des renseignements personnels sur la santé (RPS) à l'aide d'une **technologie de gestion d'identité locale** :

- le système de contrôle de l'accès et de gestion d'identité du DRS (les « services de gestion d'identité ») qui gère les processus d'authentification et d'autorisation donnant accès à [la solution de DSE] (solution de service d'émission de jetons de sécurité de [la solution de DSE], Active Directory Federation Services 2.0 de Microsoft ou autre);

- toute connexion directe au portail du fournisseur de [la solution de DSE] et aux fonctions administratives de cette dernière, ce qui comprend les composants connectés (pare-feu, serveur mandataire, etc.);

- l'intégration du portail du fournisseur de [la solution de DSE] au système d'information local du DRS ou à l'application de gestion des dossiers médicaux électroniques.

Elle vise plutôt les éléments suivants dans le cas des DRS qui utilisent [la solution de DSE] pour voir, traiter ou autrement manipuler des RPS à l'aide du **service ONE ID de Santé Ontario** :

- toute connexion directe aux fonctions administratives de [la solution de DSE], ce qui comprend les composants connectés (pare-feu, serveur mandataire, etc.).

Dans le cas des DRS qui créent et versent des RPS dans le dépôt de données cliniques de [la solution de DSE], la présente politique, en plus de ce qui est prévu pour les sites qui ne font que consulter les données, s'applique aux éléments suivants :

- les terminaux d'envoi de données qui fournissent des RPS au dépôt de données cliniques de [la solution de DSE];

- les technologies de l'information et les processus qui assurent la qualité des données envoyées (la mise en correspondance de la terminologie, par exemple).

La norme ne s'applique pas aux DRS, à leurs mandataires et à leurs fournisseurs de services électroniques qui ne créent pas, ne versent pas et ne consultent pas de données dans [la solution de DSE] et qui n'accèdent pas à cette dernière.

Définitions

[la solution de DSE] : Solution utilisée, y compris les systèmes connexes, pour stocker et rendre accessibles les renseignements personnels sur la santé contenus dans les systèmes de renseignements électroniques sur la santé des dépositaires de renseignements sur la santé.

[La solution de DSE] inclut les portails et les applications pour les patients (affiliés ou non à un dépositaire de renseignements sur la santé) qui facilitent l'accès du patient au DSE. Ces applications peuvent être :

- Commandées par le fournisseur (le fournisseur facilite la communication avec le patient)
- Fournies directement au patient (le patient a un accès direct au DSE)
- Commandées par le patient (le patient délègue l'accès à un mandataire spécial ou à d'autres délégués, p. ex., un membre de la famille ou un médecin).

Équipe de [la solution de DSE] : également appelée bureau de l'équipe; comprend des agents et des fournisseurs de services électroniques qui soutiennent [la solution de DSE], y compris les activités, les initiatives et les processus associés à la protection de la vie privée et à la sécurité.

Devrait/devraient : S'utilisent lorsqu'il y a des raisons, selon les circonstances, de ne pas exécuter ce qui est proposé. La personne doit cependant comprendre les conséquences de ses actes si elle décide de ne pas adhérer à ce qui est écrit et songer à mettre en œuvre des mesures de contrôle en guise de compensation.

Doit/doivent : S'utilisent dans le cas des exigences absolues où il n'y a aucune autre option possible.

Fournisseur de services électroniques : Personne ou entité qui fournit des biens ou des services dans le but de permettre à un dépositaire de renseignements sur la santé d'employer des moyens électroniques de recueillir, d'utiliser, de modifier, de diffuser, de conserver ou d'éliminer des renseignements personnels sur la santé et qui comprend un fournisseur de réseau d'information sur la santé.

Organisme de surveillance compétent : L'organisme de surveillance compétent est formé de cadres supérieurs qui supervisent tous les aspects liés à la [solution DSE]. Voir la section intitulée Structure de la politique de gouvernance dans le document Politique de sécurité de l'information.

Peut/peuvent : S'utilisent lorsque ce qui est proposé n'est qu'une recommandation ou ne sert que d'exemple qui ne se veut pas exhaustif.

Service de gestion d'identité : Technologies et services, politiques, processus et procédures connexes servant à créer, à conserver, à mettre en sécurité, à valider, à affirmer et à gérer des identités électroniques pour [la solution de DSE].

Système d'information : Ensemble autonome de technologies de l'information organisées de manière à recueillir, à traiter, à conserver, à utiliser, à divulguer ou à éliminer l'information.

Technologie de l'information : Tout élément (matériel ou électronique) utilisé pour l'acquisition, le stockage, la manipulation, la gestion, le déplacement, le contrôle, l'affichage, l'échange, l'envoi ou la réception automatiques de données ou d'information. Comprend, sans s'y limiter, le matériel informatique, les logiciels, les microprogrammes, le matériel auxiliaire et les ressources connexes.

Terminal d'envoi de données : Technologies et processus connexes qui alimentent le dépôt de données cliniques et font l'objet des recherches de données par l'utilisateur en milieu clinique. Comprend habituellement le système d'information (système d'information hospitalier, système d'information de laboratoire, système d'information clinique, etc.) qui se branche automatiquement à [la solution de DSE] pour rendre les données cliniques accessibles.

Exigences de la norme

1. Exigences pour les dépositaires de renseignements sur la santé

1.1. Les dépositaires de renseignements sur la santé (DRS) doivent mettre en place des périmètres de sécurité physiques pour protéger les services de gestion d'identité et les terminaux d'envoi de données de tout accès physique non autorisé et de tout dégât environnemental.

1.2. Les DRS devraient veiller à ce que les installations névralgiques (les bâtiments et les zones d'entreposage où se trouvent les services de gestion d'identité et les terminaux d'envoi de données) soient protégées contre tout accès physique non autorisé. Les méthodes pour prévenir l'accès physique peuvent être parmi les suivantes :

1.2.1. installer des verrous ou des écrous aux portes et aux fenêtres vulnérables;

1.2.2. installer un système de surveillance avec téléviseur en circuit fermé;

1.2.3. faire appel à des gardiens de sécurité;

1.2.4. installer des systèmes de détection d'intrus sur les portes extérieures et mettre à l'épreuve les fenêtres accessibles régulièrement.

1.3. Les DRS doivent veiller à ce que les installations névralgiques où se trouvent les services de gestion d'identité et les terminaux d'envoi de données ne soient pas accessibles au public. L'information sur les installations névralgiques doit demeurer confidentielle (par l'utilisation de panneaux discrets ou l'exclusion de l'information des répertoires ou bottins téléphoniques, par exemple).

1.4. Les DRS devraient veiller à ce que les personnes qui visitent les installations névralgiques respectent les conditions suivantes :

1.4.1. l'accès physique n'est permis qu'aux fins expressément autorisées;

1.4.2. elles doivent consigner leur heure d'arrivée et de départ;

1.4.3. elles sont obligées de porter un badge pour visiteur en tout temps;

1.4.4. elles font l'objet d'une constante surveillance;

1.4.5. on les informe sur ce qu'elles ne peuvent pas faire (filmer ou prendre des photos, par exemple).

Services publics et environnement

1.5. Les DRS devraient veiller à ce que les terminaux d'envoi de données et les services de gestion d'identité soient protégés des pannes d'électricité et d'autres sources de perturbations causées par les services publics et l'environnement (électricité, eau courante, chauffage, aération ou climatisation, par exemple).

1.6. Les DRS devraient veiller à ce que les fils électriques qui parviennent aux installations névralgiques qui abritent des terminaux d'envoi de données et des services de gestion d'identité soient protégés. Les méthodes de protection peuvent être parmi les suivantes :

1.6.1. séparer les fils électriques des fils de services de télécommunications pour empêcher les interférences;

1.6.2. les installer de manière à ce qu'ils ne soient pas visibles;

1.6.3. opter pour des mécanismes de verrouillage aux points d'inspection et aux extrémités;

1.6.4. opter pour d'autres modes d'alimentation électronique ou d'autres voies pour les fils;

1.6.5. éviter de passer par des zones publiques.

1.7. Les DRS doivent veiller à ce que l'alimentation électronique des terminaux d'envoi de données et des services de gestion d'identité soit protégée et satisfaire aux exigences des fabricants. Les méthodes de protection peuvent être parmi les suivantes :

1.7.1. employer un dispositif d'alimentation sans coupure qui possède une pile assez forte pour la mise hors fonction du système;

1.7.2. installer un limiteur de surtension;

1.7.3. avoir des génératrices d'urgence en cas de panne prolongée;

1.7.4. installer un éclairage d'urgence en cas de panne générale;

1.7.5. connaître l'emplacement des interrupteurs de mise hors tension près des sorties d'urgence pour faciliter et accélérer la mise hors tension pendant une urgence;

1.7.6. respecter les exigences de climatisation, de chauffage, d'humidité et de qualité de l'air des fabricants.

Câbles de télécommunications

1.8. Les câbles de télécommunications servant à transmettre l'information nécessaire aux terminaux d'envoi de données et aux services de gestion d'identité doivent être protégés contre toute interruption ou tout bris. Les méthodes de protection peuvent être parmi les suivantes :

1.8.1. installer une gaine renforcée ainsi que des chambres ou des boîtiers verrouillés aux points d'inspection et aux extrémités;

1.8.2. utiliser d'autres voies ou d'autres supports de transmission;

1.8.3. utiliser des câbles de fibre optique;

1.8.4. utiliser une protection électromagnétique pour les câbles;

1.8.5. placer des liaisons redondantes;

1.8.6. effectuer des balayages techniques et des inspections physiques d'appareils non autorisés branchés aux câbles;

1.8.7. limiter l'accès aux tableaux de connexions et aux salles de câblages.

Protection contre les catastrophes

1.9. Les DRS devraient veiller à ce que les installations névralgiques abritant des terminaux d'envoi de données et des services de gestion d'identité soient protégées des catastrophes d'origine naturelle ou humaine (dans une zone à faible risque d'inondation, d'incendie, d'explosion ou de bris causés par des activités du milieu environnant, par exemple).

1.10. Les DRS devraient réduire au minimum l'effet des catastrophes sur les installations névralgiques abritant des terminaux d'envoi de données et des services de gestion d'identité par les moyens suivants :

1.10.1. repérer les extincteurs d'incendie pour qu'on règle les incidents mineurs sans délai;

1.10.2. montrer aux mandataires, et au besoin aux fournisseurs de services électroniques, comment utiliser l'équipement en cas d'urgence (comme les extincteurs) et quelles sont les procédures d'évacuation;

1.10.3. surveiller et contrôler la température et l'humidité.

1.11. Les DRS devraient veiller à ce que les alarmes d'incendie dans les installations névralgiques soient constamment sous surveillance et régulièrement testées et entretenues conformément aux exigences du fabricant.

Centres de données

1.12. Les DRS devraient veiller à ce que les centres de données existants et ceux acquis par location, achat ou construction abritant des terminaux d'envoi de données et des services de gestion d'identité fassent l'objet d'un examen périodique pour assurer les contrôles de sécurité physiques qui protègent l'information stockée ou traitée dans le centre de données.

1.13. Les DRS devraient superposer des zones à mesures de sécurité matérielles dans les centres de données où se trouvent des terminaux d'envoi de données et des services de gestion d'identité pour assurer une protection de fond en comble.

1.14. Les DRS doivent veiller à ce que les points d'accès physique dans les centres de données abritant des terminaux d'envoi de données et des services de gestion d'identité, notamment les zones de livraison ou de chargement, ou toute autre zone où du personnel non autorisé peut entrer dans les locaux, fassent l'objet d'un contrôle et, si possible, qu'ils demeurent isolés des zones où se trouvent les systèmes d'information névralgiques pour éviter tout accès physique non autorisé.

1.15. Les DRS devraient exiger de leurs mandataires et de leurs fournisseurs de services électroniques qu'ils obtiennent une approbation avant de quitter les centres de données avec des technologies utilisées pour le fonctionnement des services de gestion d'identité et des terminaux d'envoi de données.

2. Exigences pour l'équipe de [la solution de DSE]

2.1. L'équipe de [la solution de DSE] doit mettre en place des périmètres de sécurité physiques pour protéger les composants de [la solution de DSE] de tout accès physique non autorisé et de tout dégât environnemental.

2.2. L'équipe de [la solution de DSE] doit veiller à ce que la force de chaque périmètre dépende des exigences de sécurité physique pour les renseignements et les technologies de l'information qui se trouvent à l'intérieur du périmètre et, au besoin des résultats d'une évaluation des menaces et des risques.

2.3. L'équipe de [la solution de DSE] doit veiller à ce que les installations névralgiques (les bâtiments et les zones d'entreposage où se trouvent les systèmes d'information qui stockent ou traitent des renseignements personnels sur la santé [RPS] ou de l'information restreinte) soient protégées contre tout accès physique non autorisé. Les méthodes pour prévenir l'accès physique peuvent être parmi les suivantes :

2.3.1. installer des verrous ou des écrous aux portes et aux fenêtres vulnérables;

2.3.2. installer un système de surveillance avec téléviseur en circuit fermé;

2.3.3. faire appel à des gardiens de sécurité;

2.3.4. installer des systèmes de détection d'intrus sur les portes extérieures et mettre à l'épreuve les fenêtres accessibles régulièrement.

2.4. L'équipe de [la solution de DSE] doit veiller à ce que les installations névralgiques soient situées loin zones facilement accessibles au public. L'information sur les installations névralgiques doit demeurer confidentielle (par l'utilisation de panneaux discrets ou l'exclusion de l'information des répertoires ou bottins téléphoniques, par exemple).

2.5. L'équipe de [la solution de DSE] devrait veiller à ce que les personnes qui visitent les installations névralgiques respectent les conditions suivantes :

2.5.1. l'accès physique n'est permis qu'aux fins expressément autorisées;

2.5.2. elles doivent consigner leur heure d'arrivée et de départ;

2.5.3. elles sont obligées de porter un badge pour visiteur en tout temps;

2.5.4. elles font l'objet d'une constante surveillance;

2.5.5. on les informe sur ce qu'elles ne peuvent pas faire (filmer ou prendre des photos, par exemple).

Services publics et environnement

2.6. L'équipe de [la solution de DSE] doit veiller à ce que les systèmes d'information névralgiques (ceux qui stockent ou traitent des RPS ou de l'information restreinte, par exemple) soient protégés des pannes d'électricité et d'autres sources de perturbations causées par les services publics et l'environnement (électricité, eau courante, chauffage, aération ou climatisation, par exemple).

2.7. L'équipe de [la solution de DSE] doit veiller à ce que les fils électriques qui parviennent aux installations névralgiques soient protégés. Les méthodes de protection peuvent être parmi les suivantes :

2.7.1. séparer les fils électriques des fils de services de télécommunications pour empêcher les interférences;

2.7.2. les installer de manière à ce qu'ils ne soient pas visibles;

2.7.3. opter pour des mécanismes de verrouillage aux points d'inspection et aux extrémités;

2.7.4. opter pour d'autres modes d'alimentation électronique ou d'autres voies pour les fils;

2.7.5. éviter de passer par des zones publiques.

2.8. L'équipe de [la solution de DSE] doit veiller à ce que l'alimentation électrique des installations névralgiques soit protégée. Les méthodes de protection peuvent être parmi les suivantes :

2.8.1. employer un dispositif d'alimentation sans coupure qui possède une pile assez forte pour la mise hors fonction des systèmes d'information névralgiques;

2.8.2. installer un limiteur de surtension;

2.8.3. avoir des génératrices d'urgence en cas de panne prolongée;

2.8.4. installer un éclairage d'urgence en cas de panne générale;

2.8.5. connaître l'emplacement des interrupteurs de mise hors tension près des sorties d'urgence pour faciliter et accélérer la mise hors tension pendant une urgence;

2.8.6. respecter les exigences de climatisation, de chauffage, d'humidité et de qualité de l'air des fabricants.

Câbles de télécommunications

2.9. L'équipe de [la solution de DSE] doit veiller à ce que les câbles de télécommunications qui transmettent l'information nécessaire à [la solution de DSE] soient protégés contre toute interruption ou tout bris. Les méthodes de protection peuvent être parmi les suivantes :

2.9.1. installer une gaine renforcée ainsi que des chambres ou des boîtiers verrouillés aux points d'inspection et aux extrémités;

2.9.2. utiliser d'autres voies ou d'autres supports de transmission;

2.9.3. utiliser des câbles de fibre optique;

2.9.4. utiliser une protection électromagnétique pour les câbles;

2.9.5. placer des liaisons redondantes;

2.9.6. effectuer des balayages techniques et des inspections physiques d'appareils non autorisés branchés aux câbles;

2.9.7. limiter l'accès aux tableaux de connexions et aux salles de câblages.

2.10. L'équipe de [la solution de DSE] devrait veiller à ce que l'équipement de télécommunications soit branché d'au moins deux manières différentes au service public pour éviter les interruptions de service.

Protection contre les catastrophes

2.11. L'équipe de [la solution de DSE] doit veiller à ce que les installations névralgiques soient protégées des catastrophes d'origine naturelle ou humaine (dans une zone à faible risque d'inondation, d'incendie, d'explosion ou de bris causés par des activités du milieu environnant, par exemple).

2.12. L'équipe de [la solution de DSE] doit réduire au minimum l'effet des catastrophes sur les installations névralgiques par les moyens suivants :

2.12.1. repérer les extincteurs d'incendie pour qu'on règle les incidents mineurs sans délai;

2.12.2. montrer aux mandataires, et au besoin aux fournisseurs de services électroniques, comment utiliser l'équipement en cas d'urgence (comme les extincteurs) et quelles sont les procédures d'évacuation;

2.12.3. surveiller et contrôler la température et l'humidité.

2.13. L'équipe de [la solution de DSE] doit veiller à ce que les alarmes d'incendie dans les installations névralgiques soient constamment sous surveillance et régulièrement testées et entretenues conformément aux exigences du fabricant.

Centres de données

2.14. L'équipe de [la solution de DSE] doit veiller à ce que les centres de données existants et ceux acquis par location, achat ou construction fassent l'objet d'un examen périodique pour assurer les contrôles de sécurité physiques qui protègent l'information stockée ou traitée dans le centre de données.

2.15. Les centres de données de l'équipe de [la solution de DSE] doivent être séparés en zones distinctes d'après les besoins opérationnels (salles des serveurs, armoires de câblage, centres d'appels, zones connexes, prestation de services, réception, etc.).

Chaque zone doit être jumelée à une zone de sécurité matérielle pour qu'on détermine les mesures de sécurité matérielles nécessaires. Les zones à mesures de sécurité matérielles ayant les mesures de contrôle matérielles minimales pour [la solution de DSE] se trouvent à l'annexe A intitulée *Zones à mesures de sécurité matérielles pour [la solution de DSE]*.

2.16. L'équipe de [la solution de DSE] doit superposer des zones à mesures de sécurité matérielles dans les centres de données pour assurer une protection de fond en comble.

S'il est impossible de le faire (en raison de la configuration d'un environnement ou de besoins opérationnels en particulier), le nombre maximal de zones qu'on peut sauter dans la conception de l'environnement d'un centre de données doit être limité à un. Dans un tel cas, l'évaluation des menaces et des risques doit tenir compte de la zone sautée et des mesures de compensation doivent être étudiées et mises en œuvre.

2.17. L'équipe de [la solution de DSE] doit veiller à ce que les points d'accès physique aux centres de données, notamment les zones de livraison ou de chargement, ou toute autre zone où du personnel non autorisé peut entrer dans les locaux, fassent l'objet d'un contrôle et, si possible, qu'ils demeurent isolés des zones où se trouvent les systèmes d'information névralgiques pour éviter tout accès physique non autorisé.

2.18. L'équipe de [la solution de DSE] doit exiger que tous les mandataires et les fournisseurs de services électroniques obtiennent l'approbation d'un cadre supérieur au sein de l'équipe avant de quitter un centre de données avec des technologies de l'information nécessaires au fonctionnement de ses systèmes d'information (des serveurs et des périphériques réseau, par exemple). Un registre de tous les éléments d'actif hors site devrait être conservé.

Dérogations Toute dérogation à la norme doit être approuvée par l'organisme de surveillance compétent, lequel l'autorisera uniquement lorsque la situation le justifie et au degré minimal nécessaire pour la justification apportée.

Consultez à cet effet l'annexe A intitulée *Demandes de dérogation aux exigences en matière de sécurité de l'information* dans la *Politique de sécurité de l'information*.

Application Tous les cas de non-respect seront examinés par l'organisme de surveillance compétent.

L'organisme de surveillance compétent a le pouvoir d'imposer les sanctions appropriées, ce qui peut inclure la cessation des ententes avec le DRS ou les fournisseurs de services électroniques ou la cessation des privilèges d'accès des mandataires, et de demander des mesures correctives.

Références

Lois

- LPRPS, art. 12 et 13 et partie V.1
- O. Reg. 329/04, art. 6

Normes internationales

- ISO/IEC 27001:2005 – Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences
- ISO/IEC 27002:2005 – Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information
- ISO/IEC 27005:2008 – Technologies de l'information – Techniques de sécurité – Gestion des risques en sécurité de l'information
- ISO 27799:2008 – Informatique de santé – Management de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002

Documents de politiques sur les DSE de Santé Ontario

- Politique de sécurité de l'information
- Politique d'utilisation acceptable des données et des technologies de l'information
- Politique sur le contrôle de l'accès aux systèmes et les processus de gestion d'identité connexes
- Politique sur les pratiques de l'autorité locale d'enregistrement
- Norme sur la fédération d'identités (en anglais)
- Politique sur la continuité des activités
- Politique sur la cryptographie
- Politique sur les fournisseurs de services électroniques
- Politique sur la gestion des incidents de sécurité de l'information
- Politique sur la gestion de l'information et des éléments d'actif
- Politique sur les réseaux et les opérations
- Politique sur la journalisation de sécurité et la surveillance
- Politique sur le cycle de développement de systèmes
- Politique sur la sécurité matérielle
- Politique sur la gestion des menaces et des risques
- Politiques harmonisées sur la protection de la vie privée (en anglais)

Annexe A : Zones à mesures de sécurité matérielles pour [la solution de DSE]

Zones	Description	Requirements
Zone publique	Est considérée comme zone publique toute entrée publique d'un bâtiment et l'environnement juste autour de l'entrée. En voici des exemples : • le stationnement d'un immeuble; • le terrain autour d'un immeuble; • tout endroit sans accès restreint pour le public pendant les heures de travail.	Il n'y a aucune exigence spéciale pour les zones publiques, car il n'est pas toujours possible de gérer de tels environnements de manière directe.
Zone de réception	Une zone de réception est une zone d'accès public où les personnes de l'extérieur ont un contact avec le personnel de l'immeuble pour des raisons administratives ou pour avoir accès à l'immeuble. En voici des exemples : • l'entrée principale d'un immeuble ou d'un étage lorsqu'il y a plus d'un locataire dans l'immeuble; • les zones où sont accueillis et attendent les visiteurs; • les comptoirs et kiosques de services publics.	• Des mesures de contrôle physique doivent être mises en place pour restreindre l'entrée des visiteurs (par un comptoir d'accueil, des gardiens ou des dispositifs d'accès physique tels que les lecteurs de cartes, par exemple). • Lorsque c'est possible, l'accès des visiteurs à la zone de réception doit être limité à certaines heures (il peut être limité dans un centre de données, mais pas dans un hôpital, par exemple). • Toute demande d'authentification ou d'approbation pour accéder à l'immeuble (présentation de cartes ou validation de l'accès, par exemple) devrait avoir lieu dans la zone de réception.
Zone d'opérations	La zone d'opérations est une zone contrôlée périodiquement ou de manière non rigoureuse dans l'immeuble où l'accès est limité au personnel autorisé et aux visiteurs approuvés ou accompagnés seulement. En voici des exemples : • les placards; • les bureaux des employés et les endroits similaires.	• Le périmètre de la zone d'opérations doit être facile à reconnaître. • Il est interdit d'accorder l'accès au public, et on devrait y retrouver des barrières physiques (murs, portes verrouillées, etc.) à cet effet. • La zone d'opérations ne doit être accessible que depuis une zone de réception et doit être séparée de la zone de réception par un mur et une porte verrouillée (à moins d'avoir obtenu une exemption conformément au point 2.17 du présent document).
Zone de sécurité	La zone de sécurité est une zone dans l'immeuble qui fait l'objet d'une surveillance continue et qui est accessible pour le personnel autorisé et les visiteurs approuvés ou accompagnés seulement. Le plancher surélevé d'un centre de	• La zone de sécurité doit avoir un périmètre facile à reconnaître et faire appel à des barrières physiques solides, fiables et hautement efficaces qui empêchent l'accès. • La zone de sécurité doit être conçue de manière à ce que les barrières et les portes demeurent continuellement

	données peut être inclus dans une zone de sécurité. Il peut y avoir d'autres zones de sécurité, par exemple les armoires de câblage névralgique.	fermées et verrouillées lorsqu'elles ne sont pas utilisées. • Il faut surveiller l'activité qui y a lieu et intervenir sur-le-champ. • L'accès doit être restreint et consigné en tout temps, par exemple par le recours à un gardien qui accorde l'accès ou l'utilisation d'un lecteur de cartes qui enregistre chaque accès. • La zone de sécurité doit être située dans une zone d'opérations (à moins d'une exemption obtenue conformément au point 2.17 du présent document).
Zone de haute sécurité	La zone de haute sécurité est une zone dans l'immeuble faisant l'objet d'une surveillance continue et n'étant accessible que pour une liste bien précise de personnes désignées et autorisées ou les visiteurs approuvés ou accompagnés par une personne désignée et autorisée. En fait partie tout environnement de traitement névralgique dédié qui doit être physiquement distinct de la zone de plancher surélevé.	• La zone de haute sécurité doit avoir un périmètre facile à reconnaître et faire appel à des barrières physiques solides, fiables et hautement efficaces qui empêchent l'accès. • La zone de haute sécurité doit être conçue de manière à ce que les barrières et les portes demeurent continuellement fermées et verrouillées lorsqu'elles ne sont pas utilisées. • Il faut surveiller l'activité qui y a lieu sans interruption et intervenir sur-le-champ. • Tout l'accès doit être restreint et consigné en tout temps, en plus de faire l'objet d'un audit au moins une fois par mois. • Les personnes qui doivent avoir accès à une zone de haute sécurité doivent subir un contrôle de sécurité et être ajoutées à une liste de personnes désignées qui ont accès à la zone. • Tous les visiteurs approuvés doivent être accompagnés en tout temps d'une personne désignée et autorisée. • La zone de haute sécurité doit être située dans une zone de sécurité (à moins d'une exemption obtenue conformément au point 2.17 du présent document).