Ontario Health

Norme sur les réseaux et les opérations

Version: 2.0

N° de document : 3544

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	2017-03-20
Connecting Security Committee	2018-03-26
Connecting Security Committee	2019-07-04
Connecting Security Committee	2021-03-18

Historique des révisions

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
1.0	2013-11-18	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	2014-05-16	Révision du contenu à la suite de la réunion du 13 mai du groupe de travail sur la protection de la vie privée et la sécurité de ConnexionRGT. Modifications apportées aux sections de gestion des correctifs, d'analyse de configuration et de gestion de la vulnérabilité.	Mark Carter
1.2	2014-10-09	Révisions 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. Reformulations dans les sections de la portée, des dérogations et de l'application aux fins d'uniformité avec les politiques du Comité ConnexionConfidentialité. Ajout d'une définition de « terminaux d'envoi de données » et de « service de gestion d'identité ». Révisions aux dérogations pour les cas où le réseau doit demeurer accessible en tout temps; ajout de références aux lignes directrices du CIS et du fournisseur pour le renforcement de la sécurité des systèmes; révision de l'option d'exécuter diverses fonctions système sur le même serveur si le niveau de sécurité est similaire; ajout d'autres possibilités pour les antivirus et la fréquence d'analyse de vulnérabilité; ajout d'options lorsqu'il est impossible de mettre à l'essai des correctifs; révision de la fréquence de l'examen des passerelles (de 6 à 12 mois); allègement du lien	Mark Carter

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
		entre évaluation de la vulnérabilité et résultats des tests d'intrusion dans les évaluations des menaces et des risques; clarification de l'approbation des outils d'analyse de vulnérabilité; révision de la fréquence des sauvegardes en fonction de la durée maximale d'interruption admissible et de la perte de données maximale admissible; révision des exigences de mise à l'essai procédures de restauration intégrale; création d'une référence à la politique de conservation du Comité ConnexionConfidentialité.	
1.3	2014-10-16	Révision à la suite de la réunion du Comité ConnexionSécurité du 15 octobre. Ajout du point 1.20 concernant les exigences d'antivirus pour les outils approuvés des DRS. Révision du point 2.13 de manière à remplacer « externe » par « un service de gestion d'identité ou un terminal d'envoi de données » lorsqu'il est question d'authentification d'éléments d'actif branchés à distance à [la solution de DSE]. Expansion du contenu sur la mise en œuvre de mesures de chiffrement au point 2.25.	Mark Carter
1.4	2014-11-26	Reformulation des exigences de renforcement de la sécurité aux points 1.7 à 1.10 pour accorder une flexibilité accrue à la suite des discussions du 5 novembre avec les membres du Comité ConnexionSécurité. Modification du point 1.26 pour permettre la réalisation d'analyses de vulnérabilité et de configuration tous les six mois. Approbation de la politique à la réunion du Comité ConnexionSécurité.	Mark Carter
1.5	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
1.6	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 processus de décision en matière de dérogation.	Mark Carter
1.7	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.	Ravi Addepalli
1.8	16 mars 2018	Mise à jour de la norme afin d'inclure l'accès au DSE par les patients.	Geovanny Diaz

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
1.9	4 juillet 2019	Mise à jour de la norme afin d'améliorer les exigences et d'éliminer les redondances.	Ravi Addepalli
2.0	2021-01-04	Examen du document avec des modifications mineures, mise à jour du modèle et du cycle de révision tous les deux ans	Ana Fukushima

Norme sur les réseaux et les opérations

Objet

La présente norme a pour but de définir les exigences d'implantation et de maintien de réseaux et de systèmes d'information sécuritaires comprenant [la solution de DSE] ainsi que de réseaux et de systèmes d'information de dépositaires de renseignements sur la santé (DRS) qui consultent des renseignements personnels sur la santé (RPS) par [la solution de DSE] ou versent des RPS dans cette dernière.

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 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.

Analyse de configuration : Processus automatique de comparaison de la configuration d'un système d'information à une configuration normale comprenant des paramètres de sécurité donnés. Les logiciels d'analyse de configuration fonctionnent généralement avec ouverture de session dans le système visé, c'est-à-dire que l'analyse se fait de l'intérieur.

Analyse des vulnérabilités : Processus automatique de détection préventive des vulnérabilités en matière de sécurité de systèmes d'information visant à déterminer si un système peut être exploité et quand il peut l'être. Les logiciels d'analyse des vulnérabilités cherchent les défauts de sécurité d'après une base de données de défauts connus et fonctionnent avec ou sans ouverture de session dans le système visé, c'est-à-dire que l'analyse se fait de l'intérieur ou de l'extérieur.

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 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, à détruire 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, moteur d'interface HL7, 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 conserver un registre des éléments d'actif associés à leurs services de gestion d'identité et à leurs terminaux d'envoi de données.

1.2. Les DRS doivent consigner et conserver les schémas du réseau englobant l'ensemble des connexions directes aux services de gestion d'identité et aux terminaux d'envoi de données. Peuvent faire partie des schémas les éléments suivants :

1.2.1. les topologies physiques et logiques;

1.2.2. la configuration des périphériques du réseau;

1.2.3. les points d'accès aux réseaux extérieurs;

1.2.4. les périphériques du réseau connectés.

Zones réseau

1.3. Les DRS doivent créer des zones réseau et gérer ces dernières de manière à tenir compte de la séparation entre les divers environnements informatiques. La séparation des réseaux peut se faire en fonction de divers facteurs, notamment :

1.3.1. le type d'information transmis sur le réseau;

1.3.2. le niveau d'assurance requis.

1.4. Les DRS doivent maintenir un contrôle sur le trafic dans les zones réseau à l'aide d'une passerelle de sécurité le long du périmètre de chaque zone.

Passerelles de sécurité

1.5. Les DRS doivent configurer leurs passerelles de sécurité de manière à ce qu'elles filtrent les mouvements vers les zones réseau et hors des zones réseau contenant leurs services de gestion d'identité et leurs terminaux d'envoi de données en refusant tout mouvement sur le réseau (dans les deux directions) par défaut et à ce qu'elles soient en mesure de se conformer aux normes de sécurité en cas de panne si le réseau doit demeurer accessible en tout temps.

1.6. Les DRS devraient mettre en œuvre un processus visant à réexaminer la configuration des passerelles de sécurité au moins une fois par année. Ce processus devrait englober les points suivants :

1.6.1. l'examen des ensembles de règles régissant les passerelles de sécurité;

1.6.2. la suppression des règles expirées ou inutiles;

1.6.3. la résolution des règles conflictuelles;

1.6.4. le retrait des objets inutilisés ou en double, par exemple un système de réseau ou un système informatique.

Connexion au réseau

1.7. Chaque fois que c'est possible, les DRS doivent désactiver les services, protocoles et ports inutiles de leurs services de gestion d'identité et de leurs terminaux d'envoi de données. Il faut le faire chaque fois que de nouveaux systèmes sont en place ou qu'on apporte des mises à niveau importantes aux systèmes en place. D'autres configurations sont acceptables lorsque les systèmes périmétriques utilisent des listes de contrôle de l'accès ou des règles de pare-feu qui limitent l'accès aux services sur des systèmes en place sensibles aux mises à niveau. Les DRS devraient consigner et conserver les raisons justifiant l'utilisation de tous les services, protocoles et ports permis, y compris les dispositifs de sécurité prévus pour les services, protocoles et ports jugés non sécuritaires (FTP, Telnet, POP3, IMAP ou SNMP, par exemple). Les DRS devraient adhérer aux spécifications du fournisseur et aux normes de l'industrie, notamment celles du Center for Internet Security des États-Unis.

1.8. Lorsque c'est possible, les DRS doivent restreindre l'accès aux fonctions administratives des services de gestion d'identité et des terminaux d'envoi de données liés à la participation à [la solution de DSE] aux services ou aux postes de travail explicitement autorisés. Il faut le faire chaque fois que de nouveaux systèmes sont en place ou qu'on apporte des mises à niveau importantes aux systèmes en place.

Renforcement de la sécurité des systèmes et du matériel

1.9. Lorsque c'est possible, les DRS doivent renforcer la sécurité de leurs services de gestion d'identité et de leurs terminaux d'envoi de données avant de mettre ces derniers en place dans l'environnement de production. Il faut le faire chaque fois que de nouveaux systèmes sont en place ou qu'on apporte des mises à niveau importantes aux systèmes en place. D'autres configurations sont acceptables lorsque les systèmes périmétriques utilisent des listes de contrôle de l'accès ou des règles de pare-feu qui limitent l'accès aux services sur des systèmes en place sensibles aux mises à niveau. Les systèmes d'exploitation et les applications doivent être mis à niveau avant la fin du cycle de soutien. Tout système qui ne peut être mis à niveau et qui a atteint la fin de son cycle de soutien doit être considéré comme obsolète.

1.10. Lorsque c'est possible, les DRS doivent éliminer les éléments inutiles (lecteurs, fonctions, sous-systèmes ou systèmes de fichiers, par exemple) de leurs services de gestion d'identité et de leurs terminaux d'envoi de données. Il faut le faire chaque fois que de nouveaux systèmes sont en place ou qu'on apporte des mises à niveau importantes aux systèmes en place. D'autres configurations sont acceptables lorsque les systèmes périmétriques utilisent des listes de contrôle de l'accès ou des règles de pare-feu qui limitent l'accès aux services sur des systèmes en place sensibles aux mises à niveau.

Serveurs

Détection et prévention des intrusions

1.11. Les DRS doivent mettre en œuvre des mécanismes de détection ou de prévention des intrusions (des systèmes de détection et de prévention des intrusions au niveau de l'hôte et des intrusions au niveau du réseau, des outils de gestion de l'information et des événements de sécurité et des alertes automatiques) dans leurs services de gestion d'identité, leurs terminaux d'envoi de données et les appareils des utilisateurs finaux de la solution DSE.

1.12. Les DRS devraient protéger leurs capteurs de détection et de prévention des intrusions (soit le matériel utilisé pour cerner les présences non autorisées sur le réseau) contre les attaques, par exemple à l'aide d'un TAP qui cache la présence d'un capteur.

1.13. Les DRS doivent mettre à jour le logiciel de détection et de prévention des intrusions dans les délais prévus et aux moments recommandés par le fournisseur (à la découverte d'une grave vulnérabilité, par exemple).

1.14. Les DRS doivent configurer leur logiciel de détection et de prévention des intrusions de manière à ce qu'il y ait alarme ou alerte lorsqu'une activité suspecte est détectée.

1.15. Les DRS doivent configurer des seuils d'alarme ou d'alerte à partir desquels seront signalés les événements de détection ou de prévention des intrusions ou les violations de leurs politiques de protection des renseignements.

1.16. Les DRS doivent intervenir en cas d'incident de sécurité de l'information relevé par des mécanismes de détection et de prévention des intrusions conformément à leur procédure de traitement des incidents de sécurité de l'information.

Protection contre les programmes malveillants

1.17. Les DRS doivent mettre en place un logiciel de détection de programmes malveillants et de réparation ou une solution équivalente dans leurs services de gestion d'identité et leurs terminaux d'envoi de données pour les protéger des programmes malveillants. Il est aussi possible d'utiliser une liste blanche d'applications ou de mettre en place la version légère d'un client pour restreindre les fonctions accessibles en écriture. Toute question quant à la possibilité de recourir à une autre solution doit être adressée au chef de la sécurité de [la solution de DSE] qui pourrait avoir à la présenter au comité de sécurité informatique.

1.18. Les DRS doivent mettre à jour toutes les semaines leurs fichiers de définitions de virus dans leurs services de gestion d'identité et leurs terminaux d'envoi de données.

1.19. Les DRS doivent maintenir à jour leur logiciel de détection des programmes malveillants et de réparation.

1.20. Les DRS doivent programmer leur logiciel de détection de programmes malveillants et de réparation dans leurs services de gestion d'identité et leurs terminaux d'envoi de données de manière à ce qu'ils s'exécutent à des intervalles réguliers.

Gestion des vulnérabilités

1.21. Les DRS devraient mettre en œuvre un processus de gestion des vulnérabilités portant sur les points suivants :

1.21.1. les activités d'analyse et de surveillance;

1.21.2. l'évaluation de risques;

1.21.3. l'atténuation des risques.

1.22. Les DRS devraient effectuer des analyses de vulnérabilités et de configuration de leurs services de gestion d'identité et de leurs terminaux d'envoi de données liés à [la solution de DSE] tous les six mois.

1.23. Les DRS devraient définir les délais d'intervention suivant un avis de vulnérabilité potentielle.

1.24. Les DRS doivent évaluer tous les risques qu'entraînent les vulnérabilités détectées dans leurs services de gestion d'identité et leurs terminaux d'envoi de données.

Gestion des correctifs de sécurité

1.25. En cas de correctif, les DRS doivent déterminer les risques associés à l'installation et à la non-installation de ce dernier dans leurs services de gestion d'identité et leurs terminaux d'envoi de données pour réduire rapidement les risques de vulnérabilité très élevés.

1.26. Lorsque c'est possible, les DRS doivent tester et évaluer tous les correctifs avant leur installation dans les services de gestion d'identité et leurs terminaux d'envoi de données pour en vérifier l'efficacité et voir si l'installation entraîne des conséquences néfastes pour leur organisation.

1.27. Si un DRS décide de ne pas installer un correctif dans ses services de gestion d'identité et ses terminaux d'envoi de données, il doit consigner sa décision et devrait apporter les changements en conséquence aux registres d'éléments d'actif et aux plans de continuité des activités.

1.28. Si aucun correctif n'est offert ou qu'on décide de ne pas installer un correctif dans les services de gestion d'identité ou les terminaux d'envoi de données, les DRS doivent étudier la possibilité de mettre en œuvre des mesures de contrôle pour réduire les risques qu'entraîne la vulnérabilité des systèmes. Peuvent faire partie des mesures de contrôle :

1.28.1. éteindre les services ou les fonctions exposés à la vulnérabilité;

1.28.2. adapter ou ajouter des mesures de contrôle de l'accès (pare-feu à l'entrée du réseau, par exemple);

1.28.3. augmenter la surveillance pour détecter ou empêcher les attaques.

1.29. Les DRS devraient mettre à jour la configuration ou les normes de configuration de sécurité de base de leurs services de gestion d'identité et de leurs terminaux d'envoi de données selon les besoins pour améliorer leur efficacité en fonction des résultats des analyses de vulnérabilités et de configuration.

Contrôle des changements

1.30. Les DRS doivent veiller à ce que tous les changements apportés à leurs services de gestion d'identité et à leurs terminaux d'envoi de données adhèrent à leurs procédures de contrôle des changements.

Sauvegardes

1.31. Les DRS devraient faire une sauvegarde des systèmes d'information qu'ils utilisent.

1.32. Les DRS doivent mettre en sécurité toutes les sauvegardes contenant des renseignements personnels sur la santé (RPS). Tout transfert physique de données d'un site à l'autre doit être chiffré.

1.33. Les DRS devraient régulièrement mettre à l'essai les supports de sauvegarde pour vérifier s'ils sont utilisables en cas d'urgence. Les procédures de restauration intégrale des systèmes devraient être testées une fois par année.

1.34. Les DRS devraient régulièrement mettre à l'essai leurs procédures de restauration pour vérifier si elles fonctionnent bien et si elles se font dans les délais de remise en marche prévus dans les procédures opérationnelles. Les procédures de restauration devraient être testées une fois par année.

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

2.1. L'équipe de [la solution de DSE] doit conserver un registre des technologies de l'information comprenant [la solution de DSE]. Le répertoire des éléments d'actif doit inclure, sans s'y limiter :

2.1.1. le type d'élément d'actif;

2.1.2. la propriétaire de la technologie de l'information, le cas échéant;

2.1.3. l'emplacement de la technologie de l'information (et du propriétaire, le cas échéant);

2.1.4. l'information sur les sauvegardes.

2.2. L'équipe de [la solution de DSE] doit consigner et conserver les schémas du réseau englobant l'ensemble des connexions directes à [la solution de DSE]. Peuvent faire partie des schémas les éléments suivants :

2.2.1. les topologies physiques et logiques;

2.2.2. la configuration des périphériques du réseau;

2.2.3. les points d'accès aux réseaux extérieurs;

2.2.4. les périphériques du réseau connectés.

2.3. L'équipe de [la solution de DSE] doit consigner et conserver les procédures opérationnelles pour [la solution de DSE]. Les procédures opérationnelles devraient contenir les directives détaillées des différentes tâches à exécuter, par exemple les sauvegardes, les redémarrages, les reprises informatiques et le traitement des erreurs.

2.4. L'équipe de [la solution de DSE] doit restreindre l'accès aux documents des systèmes et aux procédures opérationnelles selon les principes de privilège minimal et de besoin de savoir.

2.5. L'équipe de [la solution de DSE] devrait séparer les tâches et responsabilités de gestion de son réseau de manière à réduire les risques d'accès, de collecte, d'utilisation, de divulgation, de transfert, de modification ou de suppression non autorisés ou non intentionnels.

Zones réseau

2.6. L'équipe de [la solution de DSE] doit créer des zones réseau et gérer ces dernières de manière à tenir compte de la séparation entre les divers environnements informatiques. La séparation des réseaux devrait se faire en fonction de divers facteurs, notamment :

2.6.1. le type d'information transmis sur le réseau;

2.6.2. le niveau d'assurance requis.

2.7. L'équipe de [la solution de DSE] doit veiller à la séparation logique et physique des réseaux, c'est-à-dire de [la solution de DSE], des systèmes d'information des DRS et des réseaux publics.

2.8. L'équipe de [la solution de DSE] doit maintenir un contrôle sur le trafic dans les zones réseau à l'aide d'une passerelle de sécurité le long du périmètre de chaque zone.

Passerelles de sécurité

2.9. L'équipe de [la solution de DSE] doit configurer ses passerelles de sécurité de manière à ce qu'elles filtrent les mouvements entre les zones réseau en refusant tout mouvement sur le réseau (dans les deux directions) par défaut et à ce qu'elles soient en mesure de se conformer aux normes de sécurité en cas de panne si le réseau doit demeurer accessible en tout temps.

2.10. L'équipe de [la solution de DSE] devrait mettre en œuvre un processus visant à réexaminer la configuration des passerelles de sécurité au moins une fois par année. Ce processus devrait englober les points suivants :

2.10.1. l'examen des ensembles de règles régissant les passerelles de sécurité;

2.10.2. la suppression des règles expirées ou inutiles;

2.10.3. la résolution des règles conflictuelles;

2.10.4. le retrait des objets inutilisés ou en double, par exemple un système de réseau ou un système informatique.

Connexion au réseau

2.11. L'équipe de [la solution de DSE] doit veiller à ce que des processus d'authentification et d'autorisation soient en place sur le réseau de [la solution de DSE] avant que soit accordé l'accès à [la solution de DSE].

2.12. L'équipe de [la solution de DSE] doit veiller à ce que toute connexion à [la solution de DSE] soit sûre de manière à assurer la confidentialité et l'intégrité des RPS transmis (au moyen d'un protocole TLS, d'un RPV ou de terminaux, par exemple).

2.13. L'équipe de [la solution de DSE] doit exiger un identifiant qu'elle a elle-même approuvé (certificat numérique, adresse MAC ou adresse IP, par exemple) servant à indiquer si un service de gestion d'identité ou un terminal d'envoi de données a l'autorisation de se connecter au réseau et à déterminer à quelle zone réseau l'élément peut se connecter. La même réflexion devrait être faite pour les autres éléments connectés à [la solution de DSE].

2.14. L'équipe de [la solution de DSE] doit désactiver tous les services, protocoles et ports inutiles dans ses systèmes d'information. L'équipe de [la solution de DSE] devrait consigner et conserver les raisons justifiant l'utilisation de tous les services, protocoles et ports permis, y compris les dispositifs de sécurité prévus pour les services, protocoles et ports jugés non sécuritaires (FTP, Telnet, POP3, IMAP ou SNMP, par exemple). L'équipe de [la solution de DSE] devrait adhérer aux spécifications du fournisseur et aux normes de l'industrie, notamment celles du Center for Internet Security des États-Unis.

2.15. L'équipe de [la solution de DSE] doit mettre fin à toute connexion extérieure directe (dans l'un ou l'autre des deux sens) dans une zone réseau qui n'est pas entièrement sécurisée (une zone démilitarisée, par exemple).

2.16. L'équipe de [la solution de DSE] doit veiller à ce que tous les composants de ses systèmes d'information qui stockent des renseignements internes ou de haute importance soient situés dans une zone réseau interne séparée de la zone démilitarisée et d'autres réseaux non sécurisés.

2.17. L'équipe de [la solution de DSE] doit désactiver la séparation des flux dans tout système d'information ou toute technologie de l'information ayant accès à [la solution de DSE], sauf dans le cas des appareils de réseautage (les routeurs et les pare-feu, par exemple).

2.18. L'équipe de [la solution de DSE] devrait fermer la connexion au réseau une fois le seuil de tentatives infructueuses atteint.

2.19. L'équipe de [la solution de DSE] devrait mettre en œuvre des contrôles sur l'acheminement des données selon des mécanismes de vérification certaine de l'adresse d'origine et de l'adresse de destination.

Renforcement de la sécurité des systèmes et du matériel

2.20. L'équipe de [la solution de DSE] doit renforcer la sécurité de ses systèmes d'information avant de mettre ces derniers en place dans l'environnement de production.

2.21. L'équipe de [la solution de DSE] doit éliminer les éléments inutiles (lecteurs, fonctions, sous-systèmes, systèmes de fichiers ou serveurs Web, par exemple).

2.22. L'équipe de [la solution de DSE] doit mettre en œuvre des dispositifs de protection de l'information pour les services, protocoles ou démons essentiels, mais jugés non sécuritaires (par l'utilisation, par exemple, de technologies telles que SSH, S-FTP, SSL ou le RPV IPSec pour protéger les services non sécuritaires comme NetBIOS, le partage de fichiers, Telnet ou le protocole FTP).

Serveurs

2.23. L'équipe de [la solution de DSE] ne devrait mettre en œuvre qu'une fonction primaire par serveur pour empêcher les fonctions exigeant des niveaux de sécurité différents de coexister sur le même serveur (par exemple, les serveurs Web et les serveurs de bases de données doivent être créés sur des serveurs différents). Si les fonctions ont le même niveau de sécurité, il peut être acceptable d'exécuter plus d'une fonction par serveur. En cas de recours à des technologies de virtualisation, seule une fonction primaire devrait être créée par composant du système virtuel.

Postes de travail

2.24. L'équipe de [la solution de DSE] doit installer un pare-feu personnel sur le poste de travail, l'ordinateur portatif et, lorsque c'est possible, les autres appareils mobiles de son mandataire ou de son fournisseur de services électroniques lorsqu'il y a connexion directe à Internet et à [la solution de DSE].

2.25. L'équipe de [la solution de DSE] doit veiller à ce que les postes de travail mobiles (utilisant un ordinateur portatif, par exemple) qui doivent travailler avec des extractions de données contenant des RPS soient munis d'un chiffrement complet ou partiel adéquatement installé. Le chiffrement complet est préférable, mais il est aussi possible d'opter pour un chiffrement visant des répertoires ou un site en particulier. Il n'est pas nécessaire d'avoir un chiffrement en période de non-utilisation lorsque les RPS demeurent sur des serveurs gérés dans un centre de données protégé (comme Citrix).

Détection et prévention des intrusions

2.26. L'équipe de [la solution de DSE] doit mettre en œuvre des mécanismes de détection et de prévention des intrusions (des systèmes de détection et de prévention des intrusions au niveau de l'hôte et des intrusions au niveau du réseau) dans ses systèmes d'information et ses réseaux.

2.27. L'équipe de [la solution de DSE] doit protéger ses capteurs de détection et de prévention des intrusions (soit le matériel utilisé pour cerner les présences non autorisées sur le réseau) contre les attaques, par exemple à l'aide d'un TAP qui cache la présence d'un capteur.

2.28. L'équipe de [la solution de DSE] doit mettre à jour le logiciel de détection et de prévention des intrusions dans les délais prévus et aux moments recommandés par le fournisseur (à la découverte d'une grave vulnérabilité, par exemple).

2.29. L'équipe de [la solution de DSE] doit configurer son logiciel de détection et de prévention des intrusions de manière à ce qu'il y ait alarme ou alerte lorsqu'une activité suspecte est détectée.

2.30. L'équipe de [la solution de DSE] doit configurer des seuils d'alarme ou d'alerte à partir desquels seront signalés les événements de détection ou de prévention des intrusions ou les violations des politiques de protection des renseignements liées à [la solution de DSE] ainsi que des procédures connexes.

2.31. L'équipe de [la solution de DSE] doit intervenir en cas d'incident de sécurité de l'information relevé par des mécanismes de détection et de prévention des intrusions conformément à sa procédure de traitement des incidents de sécurité de l'information.

Protection contre les programmes malveillants

2.32. L'équipe de [la solution de DSE] doit mettre en place un logiciel de détection des programmes malveillants et de réparation ou une solution équivalente à tous ses postes de travail (ordinateurs de bureau, ordinateurs portatifs, etc.) et sur tous ses serveurs. Il est aussi possible d'utiliser une liste blanche d'applications ou de mettre en place la version légère d'un client pour restreindre les fonctions accessibles en écriture. Toute question quant à la possibilité de recourir à une autre solution doit être adressée au chef de la sécurité de [la solution de DSE] qui pourrait avoir à la présenter au comité de sécurité informatique.

2.33. L'équipe de [la solution de DSE] doit veiller à ce que les fichiers de définitions de virus soient mis à jour toutes les semaines.

2.34. L'équipe de [la solution de DSE] doit maintenir à jour son logiciel de détection des programmes malveillants et de réparation.

2.35. L'équipe de [la solution de DSE] devrait rendre automatiques les mises à jour des fichiers de définitions de virus et mettre en place une fonction de vérification des mises à jour des postes de travail et des serveurs. Lorsque les mises à jour des fichiers de définitions de virus ne sont pas automatiques, les postes de travail et les serveurs dotés du logiciel de détection des programmes malveillants et de réparation doivent être identifiés comme tels et mis à jour manuellement.

2.36. L'équipe de [la solution de DSE] doit programmer son logiciel de détection de programmes malveillants et de réparation de manière à ce qu'il s'exécute à des intervalles réguliers, soit au minimum une fois par semaine, à moins que le logiciel effectue une analyse en temps réel. L'équipe de [la solution de DSE] doit déconnecter les systèmes d'information et les technologies de l'information infectés du réseau jusqu'à assurance qu'ils sont exempts de programmes malveillants.

2.37. L'équipe de [la solution de DSE] doit mettre en place un logiciel de détection des programmes malveillants et de réparation capable d'analyser les supports électroniques ou optiques, les fichiers entrants, les pièces jointes des courriels et les téléchargements avant toute utilisation. Les vérifications doivent être effectuées à divers endroits, notamment les serveurs de messagerie électronique et les ordinateurs de bureau.

Gestion des vulnérabilités

2.38. L'équipe de [la solution de DSE] doit établir un processus de gestion des vulnérabilités portant sur les points suivants :

2.38.1. les activités d'analyse et de surveillance;

2.38.2. l'évaluation de risques;

2.38.3. l'atténuation des risques.

2.39. L'équipe de [la solution de DSE] doit surveiller ses systèmes d'information de manière à déceler toute nouvelle vulnérabilité.

2.40. L'équipe de [la solution de DSE] doit effectuer des analyses de vulnérabilités et de configuration pour [la solution de DSE] au moins une fois par trimestre pour déterminer l'efficacité des mesures de contrôle de sécurité opérationnelles et techniques en place1.

2.41. L'équipe de [la solution de DSE] doit effectuer des tests d'intrusion au moins une fois par année pour toutes les applications branchées à Internet qui fournissent un accès aux RPS de manière à ce que ces applications n'exposent pas [la solution de DSE] à des menaces inconnues2.

2.42. Les tests d'intrusion pour les applications branchées à Internet doivent comprendre des techniques de mise à l'essai d'applications Web exécutées conformément à une série de normes officielles telles qu'OWASP Top 10 pour mettre le doigt sur les faiblesses propres à ces applications (comme les injections SQL/LDAP, les injections de code directes [cross-site scripting], le piratage de session et les fausses URL) et doivent faire l'objet d'un examen rigoureux du contenu externe.

2.43. Des analyses de configuration doivent être réalisées pour assurer la conformité à la norme de configuration de sécurité de base approuvée.

2.44. Lorsque c'est possible, l'équipe de [la solution de DSE] devrait incorporer les résultats d'analyses de vulnérabilités et de configuration dans ses évaluations des menaces et des risques pour avoir un portrait exact des risques pour [la solution de DSE].

2.45. L'équipe de [la solution de DSE] doit veiller à ce que tous les risques que représentent les vulnérabilités soient cernés pour leurs systèmes d'information et à ce que leurs plans d'atténuation des risques soient évalués par un analyste en sécurité indépendant des équipes internes.

2.46. L'équipe de [la solution de DSE] doit veiller à ce que toutes les vulnérabilités cernées dans ses systèmes d'information soient corrigées dans des délais déterminés ou doit accepter le risque qu'entraîne une vulnérabilité s'il est convenu de ne pas corriger cette dernière.

2.47. L'équipe de [la solution de DSE] devrait conserver une liste des outils d'analyse des vulnérabilités et de configuration approuvés par le chef de la sécurité de [la solution de DSE].

2.48. L'équipe de [la solution de DSE] doit définir les délais d'intervention suivant un avis de vulnérabilité potentielle.

---

[1] Voir la Politique sur le cycle de développement de systèmes pour les exigences d'analyse des vulnérabilités pour les nouveaux systèmes ou services ou de nouvelles versions de systèmes ou services.

[2] Voir la Politique sur le cycle de développement de systèmes pour les exigences relatives aux intrusions pour les nouvelles applications branchées à Internet ou de nouvelles versions d'applications.

Gestion des correctifs de sécurité

2.49. L'équipe de [la solution de DSE] doit élaborer un processus de gestion des correctifs de sécurité pour que les correctifs offerts soient connus, évalués et, lorsque la situation s'y prête, déployés. Le processus de gestion des correctifs de sécurité peut être partie intégrante d'un processus général de gestion des correctifs.

2.50. En cas de correctif, l'équipe de [la solution de DSE] doit déterminer les risques associés à l'installation de ce dernier (par une comparaison des risques de vulnérabilité du système et des risques d'installation du correctif).

2.51. Lorsque c'est possible, l'équipe de [la solution de DSE] doit mettre à l'essai et évaluer tous les correctifs avant leur installation pour en vérifier l'efficacité et voir si l'installation entraîne des conséquences néfastes pour leur organisation.

2.52. S'il est décidé de ne pas installer un correctif, l'équipe de [la solution de DSE] doit consigner sa décision et apporter les changements en conséquence aux registres d'éléments d'actif et aux plans de continuité des activités.

2.53. Si aucun correctif n'est offert ou qu'on décide de ne pas installer un correctif, l'équipe de [la solution de DSE] doit étudier la possibilité de mettre en œuvre des mesures de contrôle pour réduire les risques qu'entraîne la vulnérabilité des systèmes. Peuvent faire partie des mesures de contrôle :

2.53.1. éteindre les services ou les fonctions exposés à la vulnérabilité;

2.53.2. adapter ou ajouter des mesures de contrôle de l'accès (pare-feu à l'entrée du réseau, par exemple);

2.53.3. augmenter la surveillance pour détecter ou empêcher les attaques.

2.54. L'équipe de [la solution de DSE] doit examiner et mettre à jour la configuration de ses systèmes d'information ou les normes de configuration de sécurité de base selon les besoins pour améliorer l'efficacité des systèmes à la suite d'analyses de vulnérabilités et de changements dans les pratiques de l'industrie.

Contrôle des changements

2.55. L'équipe de [la solution de DSE] doit veiller à ce que tous les changements apportés aux réseaux et aux systèmes d'information adhèrent à ses procédures de contrôle des changements.

Sauvegardes

2.56. L'équipe de [la solution de DSE] doit effectuer une sauvegarde de [la solution de DSE] de manière à ce qu'il puisse y avoir rétablissement après une catastrophe ou une panne.

2.57. L'équipe de [la solution de DSE] doit veiller au minimum à ce qu'une sauvegarde de [la solution de DSE] soit faite conformément à la durée maximale d'interruption admissible et à la perte de données maximale admissible.

2.58. L'équipe de [la solution de DSE] doit veiller à ce que les sauvegardes soient stockées à un endroit suffisamment éloigné pour éviter tout dommage causé par une catastrophe ayant lieu au site principal.

2.59. L'équipe de [la solution de DSE] doit mettre en sécurité toutes les sauvegardes contenant des RPS. Tout transfert physique de données d'un site à l'autre doit être chiffré.

2.60. L'équipe de [la solution de DSE] doit veiller à ce que les supports de sauvegarde et les systèmes d'information soient protégés par des mesures de contrôle physique et environnemental équivalentes à celles appliquées au site principal.

2.61. L'équipe de [la solution de DSE] doit mettre à l'essai les supports de sauvegarde de manière régulière et surveiller, signaler et corriger les problèmes de sauvegarde.

2.62. L'équipe de [la solution de DSE] doit régulièrement mettre à l'essai ses procédures de restauration pour vérifier si elles fonctionnent bien et si elles se font dans les délais de remise en marche prévus dans les procédures opérationnelles. Les procédures de restauration doivent être mises à l'essai au moins une fois par année.

2.63. La période de conservation des données archivées de [la solution de DSE] doit être déterminée par les exigences à cet effet propres à la catégorie de renseignements qui y sont contenus et conformément à toute exigence légale ou réglementaire ainsi qu'à la politique harmonisée de conservation et de destruction du Comité ConnexionConfidentialité.

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)