Ontario Health

Norme sur le cycle de développement de systèmes

Version: 1.9

N° de document : 3546

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
System Development Lifecycle Standard	2017-03-30
Comité ConnexionSécurité	2018-03-26
Comité ConnexionSécurité	2020-03-31
Comité ConnexionSécurité	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 en fonction des modifications présentées par le programme ConnexionRGT le 13 mai. Révisions aux sections de la configuration et des tests d'intrusion.	Mark Carter
1.2	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 ». Amélioration de la section de la portée pour aborder la question des fournisseurs de services électroniques et des organisations qui intègrent [la solution de DSE] à leurs propres solutions. Révision de la section sur la séparation des environnements de production et autres selon la sensibilité des données. Révision de l'exigence d'évaluation des vulnérabilités et d'analyse de la configuration pour les versions importantes.	Mark Carter
1.3	2014-11-05	Approbation de la politique à la réunion du 5 novembre 2014 du Comité ConnexionSécurité.	Mark Carter

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
1.4	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
1.5	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
1.6	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
1.7	2018-03-16	Mise à jour de la norme afin d'inclure l'accès au DSE par les patients.	Geovanny Diaz
1.9	2021-04-01	Examen du document avec des modifications mineures et mise à jour du cycle de révision tous les deux ans	Ana Fukushima

Norme sur le cycle de développement de systèmes

Objet

La présente norme vise à définir les contrôles de protection de l'information nécessaires lors du développement et de l'implantation de systèmes d'information.

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 et le travail de développement effectué par les fournisseurs de services électroniques qui prennent en charge [la solution de DSE].

Elle s'applique aux organisations qui se servent de [la solution de DSE] pour intégrer les données dans leurs propres solutions.

Elle vise les éléments suivants dans le cas des dépositaires de renseignements sur la santé (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 norme, 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 ou à éliminer l'information.

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 DRS doivent effectuer des activités de développement et de test sur leurs services de gestion d'identité et les terminaux d'envoi de données dans des environnements autres que ceux de production.

1.2. Les DRS devraient mettre en œuvre des mesures de contrôle pour séparer leurs environnements de production des autres environnements. Ces mesures de contrôle peuvent inclure les suivantes :

1.2.1. employer des paramètres de contrôle de l'accès distincts;

1.2.2. utiliser du matériel informatique distinct pour les activités de production et les autres activités;

1.2.3. segmenter le réseau de production des autres réseaux (par le recours à des passerelles réseau, par exemple).

Analyse et spécification des exigences

1.3. Les DRS devraient effectuer un examen de base de la sécurité de l'information pour les mises à niveau nouvelles ou projetées de leurs services de gestion d'identité et de leurs terminaux d'envoi de données.

1.4. Les DRS devraient conserver par écrit les exigences en matière de protection de l'information de leurs services de gestion d'identité et de leurs terminaux d'envoi de données pour qu'on puisse s'en servir pour établir les exigences des futures versions des systèmes en question.

Conception

1.5. Les DRS devraient examiner les spécifications et les processus de conception des modifications nouvelles ou projetées apportées à leurs services de gestion d'identité et à leurs terminaux d'envoi de données de manière à ce qu'il y ait des mesures de contrôle suffisantes pour répondre aux exigences en matière de protection de l'information.

Développement

1.6. Les DRS devraient protéger tout code source lié à leurs services de gestion d'identité et à leurs terminaux d'envoi de données contre les modifications et les accès non autorisés (au moyen de mesures de contrôle de l'accès, par exemple).

1.7. Les DRS devraient stocker tout code source lié à leurs services de gestion d'identité et à leurs terminaux d'envoi de données dans un dépôt de codes sources et mettre en œuvre des mesures de contrôle des versions pour gérer le développement de codes.

1.8. Les DRS devraient exiger que les codes personnalisés liés à leurs services de gestion d'identité et à leurs terminaux d'envoi de données fassent l'objet d'un examen avant leur utilisation dans l'environnement de production. Les examens de codes personnalisés (les « examens de codes ») peuvent être réalisés manuellement ou avec l'aide d'outils d'examen automatisés.

1.9. Les DRS devraient veiller à ce que les déficiences ou vulnérabilités en matière de sécurité cernées pendant l'examen de codes soient corrigées ou à ce que les risques qui y sont associés soient acceptés avant leur utilisation dans un environnement de production.

Mise à l'essai

1.10. Les DRS devraient veiller à ce que les procédures de mise à l'essai des services de gestion d'identité et des terminaux d'envoi de données abordent les points suivants :

1.10.1. les types de matériel, de logiciels et de services dont il faut faire l'essai;

1.10.2. le recours à des plans d'essai structurés comprenant la contribution de l'utilisateur;

1.10.3. les types d'essais (essai de bout en bout ou test de performance, par exemple);

1.10.4. les données utilisées pour réaliser les essais;

1.10.5. la mise à l'écrit, l'analyse et l'approbation des résultats des essais.

1.11. Les DRS devraient effectuer des essais sur leurs nouveaux services de gestion d'identité et terminaux d'envoi de données en condition attendue, extraordinaire (charge excessive ou services non accessibles, par exemple) et restreinte (connexion limitée ou retard dans la réponse des services, par exemple).

Mise à l'essai des paramètres de sécurité

1.12. Les DRS devraient effectuer des analyses de vulnérabilités de leurs services de gestion d'identité et de leurs terminaux d'envoi de données de manière à déceler les faiblesses des mesures de contrôle en matière de protection de l'information et réaliser des tests d'intrusion pour voir comment on peut exploiter les vulnérabilités.

1.13. Les DRS devraient mettre en œuvre un processus pour que les failles ou les faiblesses de sécurité relevées dans le processus de mise à l'essai pour leurs services de gestion d'identité et leurs terminaux d'envoi de données soient résolues de manière cohérente.

Intégration à l'environnement de production et installation

1.14. Avant l'intégration de nouveaux services de gestion d'identité ou terminaux d'envoi de données dans l'environnement de production, les DRS devraient vérifier les points suivants :

1.14.1. les examens de sécurité de l'information ont été réalisés;

1.14.2. les limites des mesures de contrôle en matière de protection de l'information ont été consignées;

1.14.3. des ententes sur les niveaux de service ont été établies pour prendre en charge les systèmes dans l'environnement de production, le cas échéant.

1.15. Les DRS devraient déterminer et mettre en œuvre un processus d'installation ou un plan de déploiement.

1.16. Les DRS devraient créer une stratégie de reprise au point de contrôle avant de mettre en œuvre des changements.

1.17. Les DRS ne devraient permettre qu'à certains mandataires et fournisseurs de services électroniques de mettre à jour les logiciels, applications et programmathèques utilisés dans l'environnement de production.

Contrôle des changements

1.18. Les DRS devraient consigner et mettre en œuvre un processus de contrôle des changements pour tout changement apporté aux services de gestion d'identité et aux terminaux d'envoi de données de l'environnement de production.

1.19. Les DRS devraient veiller à ce que le processus de contrôle des changements réponde aux exigences suivantes :

1.19.1. conserver un registre des niveaux d'autorisation accordés;

1.19.2. veiller à ce que les changements soient présentés par des utilisateurs autorisés;

1.19.3. examiner les mesures de contrôle en matière de protection de l'information pour qu'elles ne soient pas mises en péril par les changements;

1.19.4. cerner tous les logiciels, toute l'information, toutes les entrées dans les bases de données et tout le matériel qui ont besoin de changement;

1.19.5. soumettre à l'approbation officielle du propriétaire du système d'information des propositions détaillées avant le début des travaux;

1.19.6. veiller à ce que les utilisateurs autorisés acceptent les changements avant leur mise en œuvre;

1.19.7. veiller à ce que la documentation sur le système d'information (soit les documents s'appliquant au système d'information faisant l'objet d'un changement) soit mise à jour après chaque changement et à ce que l'ancienne documentation soit archivée ou éliminée;

1.19.8. avoir en place un contrôle de versions pour toutes les mises à jour logicielles;

1.19.9. conserver un journal d'audit de toutes les demandes de changements;

1.19.10. veiller à ce que toute l'information faisant partie du processus de contrôle des changements (noms de bases de données, comptes, adresses de réseau, etc.) ne soit divulguée qu'aux parties prenantes, et ce, aux bonnes étapes de la procédure de contrôle des changements.

Examen postérieur à l'implantation

1.20. Les DRS devraient élaborer un processus de mise à l'essai des mesures de contrôle en matière de protection de l'information pour leurs systèmes d'information après leur implantation. Ce processus devrait englober les points suivants :

1.20.1. un examen des procédures de contrôle et d'intégrité des applications pour vérifier si les changements au système n'y ont pas nui;

1.21. les modifications à faire aux plans de continuité des activités.

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

2.1. L'équipe de [la solution de DSE] doit effectuer ses activités de développement et de test dans des environnements autres que ceux de production.

2.2. L'équipe de [la solution de DSE] devrait mettre en œuvre des mesures de contrôle pour séparer ses environnements de production des autres environnements tout en gardant en tête la sensibilité des données dans les environnements autres que des environnements de travail et la pratique courante. Ces mesures de contrôle peuvent inclure les suivantes :

2.2.1. employer des paramètres de contrôle de l'accès distincts;

2.2.2. utiliser du matériel informatique distinct pour les activités de production et les autres activités;

2.2.3. segmenter le réseau de production des autres réseaux (par le recours à des passerelles réseau, par exemple);

2.2.4. créer des panneaux d'avertissement distincts qui indiquent clairement l'environnement où ils se trouvent.

Analyse et spécification des exigences

2.3. L'équipe de [la solution de DSE] devrait effectuer un examen de base de la sécurité de l'information pour tous les systèmes d'information qu'elle compte utiliser en fonction des exigences connues de ces systèmes et des objectifs généraux pour imposer des exigences en matière de protection de l'information aux développeurs.

2.4. Lorsque les paramètres de sécurité de l'information d'un produit donné ne satisfont pas aux exigences en matière de protection de l'information, l'équipe de [la solution de DSE] devrait songer aux risques qui découleraient de l'intégration du système d'information avant l'achat de ce dernier.

2.5. L'équipe de [la solution de DSE] devrait consigner les exigences en matière de protection de l'information de manière à ce qu'on puisse s'y référer pour établir les exigences des futures versions du système d'information.

Conception

2.6. L'équipe de [la solution de DSE] devrait examiner les spécifications de conception de son système d'information de manière à ce qu'ils y aient des mesures de contrôle suffisantes pour répondre aux exigences en matière de protection de l'information.

2.7. L'équipe de [la solution de DSE] devrait se servir des besoins en information de l'application pour établir l'architecture du système d'information.

2.8. L'équipe de [la solution de DSE] devrait concevoir de manière détaillée chaque module, composant ou service du système d'information et consigner l'information à ce sujet. La conception détaillée devrait faire ressortir les sous-unités de l'application qui peuvent être codées, compilées et mises à l'essai.

2.9. L'équipe de [la solution de DSE] devrait concevoir de manière détaillée les interfaces extérieures au module/composant/service du système d'information, entre les composants du système d'information et entre les sous-unités de l'application et consigner l'information à ce sujet.

Développement

2.10. L'équipe de [la solution de DSE] doit protéger tout code source contre les modifications et les accès non autorisés (au moyen de mesures de contrôle de l'accès, par exemple).

2.11. L'équipe de [la solution de DSE] devrait stocker tout code source dans un dépôt de codes sources et mettre en œuvre un contrôle de versions pour gérer le développement de codes.

2.12. L'équipe de [la solution de DSE] devrait développer toutes les applications conformément aux lignes directrices sur la programmation sécuritaire. Ces lignes directrices sont accessibles auprès des entités suivantes :

2.12.1. CERT[MD];

2.12.2. le National Institute of Standards and Technology (NIST);

2.12.3. l'Open Web Application Security Project (OWASP);

2.12.4. le SANS Institute.

2.13. L'équipe de [la solution de DSE] doit veiller à ce que les comptes, les noms d'utilisateur, les clés de chiffrage privées et les mots de passe ne soient pas intégrés dans le code source ou dans la solution publiée.

2.14. L'équipe de [la solution de DSE] devrait examiner tous les codes personnalisés avant l'intégration du système dans l'environnement de production. Les examens de codes personnalisés (les « examens de codes ») peuvent être réalisés manuellement ou avec l'aide d'outils d'examen automatisés.

2.15. Tous les examens de codes manuels doivent être réalisés par des mandataires ou des fournisseurs de services électroniques autres que le développeur d'origine du code personnalisé (ou le développeur d'une firme extérieure) qui connaissent bien les techniques d'examen de codes et les pratiques de programmation sécuritaire.

2.16. Tous les examens de codes devraient cerner et corriger au minimum toutes les vulnérabilités suivantes :

2.16.1. les failles d'injection : l'examinateur de codes doit entre autres vérifier si les données insérées par un utilisateur final ne peuvent pas modifier le sens des commandes et des requêtes et utiliser des requêtes paramétrées (pour prévenir une injection SQL, une injection dans des commandes de système d'exploitation ou des failles d'injection LDAP et Xpath, par exemple);

2.16.2. les dépassements de tampon : l'examinateur de codes doit valider l'espace alloué au tampon et tronquer les chaînes d'entrée;

2.16.3. le stockage cryptographique non sécuritaire : l'examinateur de codes doit valider l'utilisation adéquate des fonctions cryptographiques qui protègent des données stockées;

2.16.4. les communications non sécurisées : l'examinateur de codes doit valider le chiffrement adéquat de toutes les communications authentifiées et sensibles;

2.16.5. les erreurs mal traitées : l'examinateur de codes doit confirmer que l'information sensible n'est pas divulguée dans les messages d'erreur.

2.17. En plus de ce qui précède, tout code personnalisé utilisé pour des applications Web et des interfaces d'application doit être mis à l'essai et corrigé dans le cas des vulnérabilités suivantes :

2.17.1. les injections XSS (cross-site scripting) : l'examinateur de codes doit entre autres valider tous les paramètres avant leur inclusion et utiliser un mécanisme d'échappement dépendant du contexte;

2.17.2. le contrôle inadéquat de l'accès : l'examinateur de codes doit confirmer que les utilisateurs finaux sont bien authentifiés, que les données entrées sont épurées, que les références aux objets internes ne sont pas exposées aux utilisateurs finaux et qu'il n'y a pas contournement des mesures de contrôle de l'accès par des portes dérobées;

2.17.3. les injections XSRF (cross-site request forgery) : l'examinateur de codes doit confirmer que les applications ne répondent pas aux jetons et autres éléments accordant des autorisations que soumettent automatiquement les fureteurs;

2.17.4. les réacheminements et les transferts invalides : l'examinateur de codes doit valider les valeurs d'URL fournies et confirmer qu'elles sont autorisées pour l'utilisateur.

2.18. L'équipe de [la solution de DSE] doit veiller à ce que toutes les failles ou vulnérabilités en matière de sécurité cernées pendant l'examen des codes soient corrigées ou que les risques qui y sont associés soient acceptés avant leur utilisation dans un environnement de production.

2.19. L'équipe de [la solution de DSE] devrait veiller à ce que les résultats de l'examen des codes soient examinés et approuvés par le gestionnaire responsable avant leur utilisation.

Développement de codes en sous-traitance

2.20. Lorsque l'accès au code source (ou l'équivalent) d'une partie extérieure est restreint, l'équipe de [la solution de DSE] devrait veiller à ce qu'une copie du code respecte les conditions suivantes :

2.20.1. elle est conservée en main tierce par une entité de confiance;

2.20.2. on vérifie régulièrement si elle est à jour et si elle fonctionne bien.

2.21. Les logiciels de fournisseurs externes devraient être utilisés sans modification (c'est-à-dire sans modification des fonctions de base de l'application).

2.22. Lorsqu'un logiciel doit être modifié, l'équipe de [la solution de DSE] devrait tenir compte des points suivants :

2.22.1. les risques de compromission des contrôles intégrés et des processus d'intégrité;

2.22.2. l'obtention auprès du fournisseur des changements nécessaires sous forme de mise à jour normale;

2.22.3. les répercussions de la responsabilité de la maintenance du logiciel à la suite des changements.

Mise à l'essai

2.23. L'équipe de [la solution de DSE] devrait veiller à ce que les procédures de mise à l'essai des systèmes d'information abordent les points suivants :

2.23.1. les types de matériel, de logiciels et de services dont il faut faire l'essai;

2.23.2. le recours à des plans d'essai structurés comprenant la contribution de l'utilisateur;

2.23.3. les types d'essais (essai de bout en bout ou test de performance, par exemple);

2.23.4. les données utilisées pour réaliser les essais;

2.23.5. la mise à l'écrit, l'analyse et l'approbation des résultats des essais.

2.24. Les nouveaux systèmes d'information devraient être mis à l'essai conformément aux plans d'essai officiels prédéfinis, lesquels devraient tenir compte des spécifications et de la conception du système d'information pour que la protection soit complète. Les représentants des principaux utilisateurs devraient participer à la planification des essais, à la soumission de données pour les essais et à l'examen des résultats des essais.

2.25. L'équipe de [la solution de DSE] devrait veiller à ce que l'environnement de mise à l'essai du système d'information reproduise l'environnement de production au plus haut degré possible.

2.26. L'ensemble de l'environnement du système d'information devrait être mis à l'essai pour cerner les conflits ou les dépendances à d'autres systèmes d'information, notamment par les moyens suivants :

2.26.1. utiliser les infrastructures de sécurité technique sous-jacentes;

2.26.2. l'interfacer sur d'autres applications;

2.26.3. employer divers systèmes d'exploitation, bibliothèques d'exécution et fureteurs;

2.26.4. l'interfacer sur des bases de données et des services de répertoire;

2.26.5. employer des configurations matérielles particulières (y compris de services, d'appareils mobiles et d'appareils portatifs).

2.27. L'équipe de [la solution de DSE] devrait effectuer des essais sur ses systèmes d'information en condition attendue, extraordinaire (charge excessive ou services non accessibles, par exemple) et restreinte (connexion limitée ou retard dans la réponse des services, par exemple).

2.28. L'équipe de [la solution de DSE] ne devrait pas utiliser de données de production à l'exception des données classées publiques dans des environnements autres que des environnements de production à moins que soient implantées dans l'environnement autre des mesures de contrôle de sécurité de l'information de même calibre que celles de l'environnement de production (ou qu'on projette d'implanter dans l'environnement de production). Sinon, l'équipe de [la solution de DSE] devrait épurer toutes les données de production (les masquer, les brouiller ou les nettoyer) avant leur chargement et leur utilisation dans des environnements autres que des environnements de production de manière à respecter les conditions suivantes :

2.28.1. il doit être impossible de retracer la personne à l'origine d'un registre ou d'une transaction;

2.28.2. l'information, si elle est divulguée à des personnes non autorisées, n'aura pas d'effet indésirable sur [la solution de DSE], ses mandataires ou ses fournisseurs de services électroniques; sur des DRS, leurs mandataires ou leurs fournisseurs de services électroniques ou sur un patient.

Mise à l'essai des paramètres de sécurité

2.29. Des activités de mise à l'essai des paramètres de sécurité devraient être intégrées lorsque c'est possible aux activités de mise à l'essai de [la solution de DSE] pour dégager de manière fréquente des données sur les améliorations à apporter en matière de protection de l'information.

2.30. L'équipe de [la solution de DSE] doit effectuer des analyses de vulnérabilités et de configuration pour chaque déploiement de nouvelles infrastructures ou nouveau service avant son intégration dans l'environnement de production, toutes les versions importantes de [la solution de DSE] faisant l'objet d'une évaluation complète des vulnérabilités.

2.31. L'équipe de [la solution de DSE] doit effectuer des tests d'intrusion pour toutes les versions majeures d'applications branchées à Internet faisant partie de [la solution de DSE] et assurant l'accès à des renseignements personnels sur la santé avant l'intégration de [la solution de DSE] dans l'environnement de production.

2.32. 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 XSS, le piratage de session et les fausses URL) et doivent faire l'objet d'un examen rigoureux du contenu externe.

2.33. L'équipe de [la solution de DSE] devrait utiliser des données d'essai préparées (haut volume d'utilisateurs simultanés, URL, entrées de lignes de commande et données aléatoires) destinées à cerner les failles ou les faiblesses (dépassements de tampon et mémoires défectueuses, par exemple) du système pour effectuer des essais de sécurité de l'information pour ses systèmes d'information.

2.34. L'équipe de [la solution de DSE] devrait élaborer un processus pour que les failles ou les faiblesses de système cernées pendant les essais soient résolues de manière uniforme comprenant les points suivants :

2.34.1. consigner l'information sur les faiblesses de sécurité détectées (dans un journal d'essai, par exemple);

2.34.2. évaluer les risques qui y sont associés;

2.34.3. mettre en œuvre des moyens de gérer ces risques;

2.34.4. répéter les essais après la mise en place des mesures correctives;

2.34.5. traiter les résultats des essais des paramètres de sécurité qui relèvent des faiblesses comme étant confidentiels jusqu'à ce que les faiblesses détectées aient été corrigées (recommandé).

2.35. Lorsque des essais des paramètres de sécurité de l'information révèlent une ou plus d'une faiblesse dans un produit de tiers, l'équipe de [la solution de DSE] devrait transmettre le résultat des essais directement au tiers.

Intégration à l'environnement de production et installation

2.36. Avant l'intégration de nouveaux systèmes d'information dans l'environnement de production, l'équipe de [la solution de DSE] doit vérifier les points suivants :

2.36.1. les examens de sécurité de l'information ont été réalisés;

2.36.2. les limites des mesures de contrôle en matière de protection de l'information ont été consignées;

2.36.3. l'approbation d'un représentant autorisé a été obtenue;

2.36.4. des ententes sur les niveaux de service ont été établies pour prendre en charge les systèmes dans l'environnement de production, le cas échéant.

2.37. L'équipe de [la solution de DSE] ne devrait pas permettre l'intégration directe du code à l'environnement de production depuis l'environnement de développement ou vice-versa, mais devrait exiger que tous les codes adhèrent à un processus d'intégration des codes.

2.38. L'équipe de [la solution de DSE] ne doit permettre que l'intégration de codes exécutables dans l'environnement de production. Les codes de développement ou compilateurs doivent être interdits dans l'environnement de production.

2.39. L'équipe de [la solution de DSE] devrait déterminer et mettre en œuvre un processus d'installation ou un plan de déploiement.

2.40. L'équipe de [la solution de DSE] devrait créer une stratégie de reprise au point de contrôle avant de mettre en œuvre des changements.

2.41. L'équipe de [la solution de DSE] devrait utiliser un système de contrôle de la configuration pour garder l'œil sur les logiciels implantés et conserver la documentation relative au système.

2.42. L'équipe de [la solution de DSE] ne devrait permettre qu'à certains mandataires et fournisseurs de services électroniques de mettre à jour les logiciels, applications et programmathèques utilisés dans l'environnement de production.

Contrôle des changements

2.43. L'équipe de [la solution de DSE] doit mettre en œuvre un processus de contrôle des changements pour gérer les changements apportés aux systèmes d'information de l'environnement de production.

2.44. L'équipe de [la solution de DSE] devrait veiller à ce que le processus de contrôle des changements réponde aux exigences suivantes :

2.44.1. conserver un registre des niveaux d'autorisation accordés;

2.44.2. veiller à ce que les changements soient présentés par des utilisateurs autorisés;

2.44.3. examiner les mesures de contrôle en matière de protection de l'information pour qu'elles ne soient pas mises en péril par les changements;

2.44.4. cerner tous les logiciels, toute l'information, toutes les entrées dans les bases de données et tout le matériel qui ont besoin de changement;

2.44.5. soumettre à l'approbation officielle du propriétaire du système d'information des propositions détaillées avant le début des travaux;

2.44.6. veiller à ce que les utilisateurs autorisés acceptent les changements avant leur mise en œuvre;

2.44.7. veiller à ce que la documentation sur le système d'information (soit les documents s'appliquant au système d'information faisant l'objet d'un changement) soit mise à jour après chaque changement et à ce que l'ancienne documentation soit archivée ou éliminée;

2.44.8. avoir en place un contrôle de versions pour toutes les mises à jour logicielles;

2.44.9. conserver un journal d'audit de toutes les demandes de changements;

2.44.10. veiller à ce que toute l'information faisant partie du processus de contrôle des changements (noms de bases de données, comptes, adresses de réseau, etc.) ne soit divulguée qu'aux parties prenantes, et ce, aux bonnes étapes de la procédure de contrôle des changements.

Examen postérieur à l'implantation

2.45. L'équipe de [la solution de DSE] doit élaborer un processus de mise à l'essai des mesures de contrôle en matière de protection de l'information pour ses systèmes d'information après leur implantation. Ce processus devrait englober les points suivants :

2.45.1. un examen des procédures de contrôle et d'intégrité des applications pour vérifier si les changements au système n'y ont pas nui;

2.45.2. les modifications à faire aux plans de continuité des activités.

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 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)

Référence à Inforoute Santé du Canada

- Exigences en matière de protection de la confidentialité et de sécurité d'Inforoute Santé du Canada (version 1.1 révisée le 7 février 2005)

Autre

- Directives concernant la sécurité des transmissions par télécopieur du commissaire à l'information et à la protection de la vie privée de l'Ontario (janvier 2003)