Ontario Health

Norme sur la gestion des incidents de sécurité de l'information

Version: 1.8

N° de document : 3539

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
Comité ConnexionSécurité	2014-09-09
Comité ConnexionSécurité	2018-03-26
Comité ConnexionSécurité	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	2014-08-18	Révisions en fonction des commentaires reçus des membres du Comité ConnexionSécurité. Révision de la section de la portée pour y inclure la mention « consulter, traiter ou autrement manipuler des renseignements personnels sur la santé (RPS) ». Révision des références à l'entente de participation; harmonisation des points 1.6 et 2.6 avec d'autres sections de la politique; révision du point 1.10 sur les options de communication; ajouts au point 1.12 pour élargir les responsabilités de signalisation au comité de protection de la vie privée et de sécurité; ajout de l'option de demander régulièrement l'état d'avancement de l'enquête au point 1.17; ajout de l'exigence de présenter les rapports d'incident au comité de protection de la vie privée et de sécurité aux points 1.20 et 2.24; harmonisation des formulations dans les sections des exceptions et de l'application.	Mark Carter
1.2	2014-09-09	Approbation de la politique à la réunion du 9 septembre 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

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
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 processus de décision en matière de dérogation.	Mark Carter
1.5	2017-03-20	Mise à jour de la norme afin de refléter l'ITRMP 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
1.7	2020-03-30	Mise a jour pout utilizer le nouveau modèle et des revisions mineurs pour clarité.	Paul Cnudde
1.8	2021-01-04	Examen du document avec des modifications mineures, mise à jour du cycle de révision tous les deux ans	Ana Fukushima

Norme sur la gestion des incidents de sécurité de l'information

Objet

La présente norme a pour but de définir les exigences liées au processus administratif de création d'un incident de sécurité de l'information (un « incident »).

Portée

La présente norme ne s'applique qu'aux incidents liés à [la solution de DSE] ou 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 dépositaires de renseignements sur la santé (DRS) qui utilisent [la solution de DSE] pour consulter, traiter ou autrement manipuler des renseignements personnels sur la santé (RPS) à l'aide d'une **technologie de gestion d'identité locale** :

- les appareils d'utilisateurs finaux servant à accéder à [la solution de DSE], y compris les fonctions administratives applicables (gestion du consentement ou rapports, par exemple);
- 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 incidents survenant aux 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** :

- les appareils d'utilisateurs finaux servant à accéder à [la solution de DSE], y compris les fonctions administratives applicables (gestion du consentement ou rapports, par exemple);
- 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 incidents survenant 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 au traitement d'incidents survenant au sein des DRS ni aux DRS, à leurs mandataires et à leurs fournisseurs de services électroniques qui ne créent pas, ne versent pas et ne consultent pas de RPS dans [la solution de DSE].

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.

Atteinte à la vie privée : Terme englobant les circonstances suivantes :

- une infraction à la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) ou son règlement a eu lieu ou est sur le point de survenir;

- les dispositions sur la protection des renseignements personnels des ententes applicables ou de toute autre entente concernant [la solution de DSE] ont été violées ou sont sur le point de l'être;

- les politiques, procédures et pratiques sur la protection des renseignements personnels mises en œuvre concernant [la solution de DSE] ont été violées ou sont sur le point de l'être;

- des renseignements personnels sur la santé dans [la solution de DSE] ont été perdus ou volés, ou une personne non autorisée a accédé ou est sur le point d'accéder à ces renseignements;

- les registres de renseignements personnels sur la santé dans [la solution de DSE] ont été copiés, modifiés ou supprimés de manière non autorisée ou sont sur le point de l'être.

Chef de la sécurité de l'information de l'équipe de [la solution de DSE] : Mandataire de l'équipe de [la solution de DSE] qui fait office de point de contact unique pour les décisions en matière de sécurité de l'information liées à [la solution de DSE].

Comité ConnexionSécurité (CCS) : La tribune provinciale sur la sécurité formée de représentants supérieurs de la sécurité provenant des régions et de Santé Ontario. C'est l'organisme décisionnaire responsable de l'établissement d'un cadre de gouvernance de la sécurité de l'information fonctionnel et utile pour les organisations participant aux DSE.

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.

Incident de sécurité de l'information : Toute violation ou menace imminente de violation des politiques, des normes, des procédures ou des pratiques de sécurité de l'information ou tout événement lié à la sécurité de l'information qui peut entraver les activités d'un système d'information ou d'un processus opérationnel ou en menacer la sécurité.

Organisme de surveillance compétent : L'organisme de surveillance compétent est formé de cadres supérieurs qui supervisent tous les aspects de 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 dépositaires de renseignements sur la santé (DRS) doivent mettre en place un processus de gestion des incidents de sécurité de l'information (les « incidents ») qui traite de toutes les phases du processus de gestion des incidents liés à [la solution de DSE] :

- détection/triage;
- intervention;
- rétablissement;
- suivi.

1.2. Si, à tout moment au cours du processus de gestion des incidents, un DRS se rend compte qu'il y a eu atteinte à la vie privée par suite de l'incident, ce dernier doit être traité conformément à la Politique de gestion des atteintes à la vie privée.

Détection/triage

1.3. Les DRS doivent établir un point de contact à qui seront signalés les incidents liés à [la solution de DSE] qui ont lieu ou dont on soupçonne l'existence. Le plus souvent, c'est le soutien technique qui fait office de point de contact.

1.4. Les DRS doivent veiller à ce que leurs mandataires et leurs fournisseurs de services électroniques sachent qu'ils doivent signaler sur-le-champ les incidents qui ont lieu ou dont on soupçonne l'existence.

1.5. Le point de contact doit créer un billet d'incident ou un journal pour tout incident lié à [la solution de DSE] signalé. Le billet d'incident doit contenir au minimum les éléments suivants :

1.5.1. l'heure et la date de l'incident signalé;

1.5.2. le nom et les coordonnées du mandataire et du fournisseur de services électroniques qui a signalé l'incident;

1.5.3. l'information relative à l'incident signalé (type et mode de détection, par exemple);

1.5.4. toutes les conséquences de l'incident signalé;

1.5.5. toutes les mesures qui sont adoptées pour limiter l'incident soivent par le mandataire ou le fournisseur de services électroniques qui a signalé l'incident, soit par le point de contact.

1.6. Les DRS doivent nommer un chef ou une équipe responsable d'effectuer les activités de triage, d'intervention, de rétablissement et de suivi des incidents relatifs à [la solution de DSE]. Le chef ou l'équipe d'intervention peut être la même personne ou la même équipe faisant office de point de contact.

1.7. Le point de contact doit envoyer tous les billets d'incidents liés à [la solution de DSE] au chef ou à l'équipe d'intervention qui sera responsable d'examiner chaque billet et les documents à l'appui pour vérifier si un incident a bel et bien eu lieu.

1.8. Le chef ou l'équipe d'intervention doit classer tous les incidents liés à [la solution de DSE] qui ont réellement eu lieu en fonction de leur gravité (voir l'annexe A intitulée *Cotes de gravité et de priorité des incidents* pour toute l'information sur les cotes de gravité).

1.9. Le chef ou l'équipe d'intervention doit entreprendre un rapport d'incident lié à [la solution de DSE] (voir l'annexe B intitulée *Contenu du rapport d'incident*).

1.10. Les DRS doivent veiller à ce que leur processus de gestion des incidents exige que le chef ou l'équipe d'intervention avise l'équipe responsable de la confidentialité et de la sécurité pour [la solution de DSE] par courriel ou téléphone et tout DRS touché au plus tard à la fin du jour ouvrable suivant les incidents confirmés au premier ou au deuxième degré de gravité conformément à l'annexe A intitulée *Cotes de gravité et de priorité des incidents*.

L'avis doit contenir au minimum les éléments suivants :

1.10.1. l'heure et la date de l'incident signalé;

1.10.2. le nom et les coordonnées du mandataire et du fournisseur de services électroniques qui a signalé l'incident;

1.10.3. l'information relative à l'incident signalé (type et mode de détection, par exemple);

1.10.4. toutes les conséquences connues ou soupçonnées de l'incident signalé;

1.10.5. toutes les mesures adoptées pour limiter l'incident soivent par le mandataire ou le fournisseur de services électroniques qui a signalé l'incident, soit par le point de contact, soit par le chef ou l'équipe d'intervention.

1.11. Si un incident qui provient d'un DRS touche plus d'un DRS ou [la solution de DSE], l'équipe de [la solution de DSE] peut diriger les activités de gestion des incidents.

1.12. L'équipe qui dirige les activités de gestion des incidents (le DRS ou l'équipe de [la solution de DSE]) doit aviser Santé Ontario, qui avisera le comité ConnexionSécurité et l'organisme de surveillance compétent dans les délais suivants :

1.12.1. dans les 72 heures suivant l'avis pour tout incident lié à [la solution de DSE] de niveau de gravité 1;

1.12.2. dans la semaine suivant l'avis pour tout incident lié à [la solution de DSE] de niveau de gravité 2.

1.13. Les DRS devraient mettre en priorité les incidents liés à [la solution de DSE] conformément à leur cote de gravité.

Intervention

1.14. Le chef ou l'équipe d'intervention doit prendre les mesures nécessaires pour limiter la portée et l'ampleur d'un incident. Les activités d'atténuation ou de confinement peuvent être les suivantes :

1.14.1. effectuer une copie de sauvegarde du système d'information;

1.14.2. cesser les activités;

1.14.3. modifier les mots de passe ou les listes de contrôle d'accès du système d'information compromis;

1.14.4. restreindre la connexion.

NOTA : Selon la gravité de l'incident, il peut être nécessaire de mettre en œuvre les plans de continuité des activités de l'organisation.

Rétablissement

1.15. Les DRS doivent rétablir les systèmes d'information touchés de manière à ce qu'ils retrouvent un état de fonctionnement normal. Les activités de rétablissement peuvent être les suivantes :

1.15.1. éliminer la cause de l'incident (suppression d'un programme malveillant, par exemple);

1.15.2. restaurer les systèmes d'information et en valider l'état;

1.15.3. décider du moment de la reprise des activités;

1.15.4. surveiller les systèmes d'information pour voir s'ils fonctionnent bien et confirmer qu'il n'y a plus de données ou de systèmes compromis.

Suivi

1.16. Les DRS doivent faire enquête à la suite d'incidents liés à [la solution de DSE] pour en déterminer la cause (par analyse par arbre de défaillances, par exemple).

1.17. Une fois un incident lié à [la solution de DSE] résolu (c'est-à-dire que toutes les activités de rétablissement ont été mises en œuvre et que les technologies de l'information et les systèmes d'information touchés sont revenus à leur état normal), le chef ou l'équipe d'intervention doit rédiger le rapport d'incident. Dans le cas des longues enquêtes menées par les DRS, l'équipe de [la solution de DSE] ou les DRS touchés doivent demander qu'on fasse le point sur l'enquête pendant le déroulement de cette dernière.

1.18. Les DRS doivent archiver leurs rapports d'incident liés à [la solution de DSE] pour au moins 24 mois.

1.19. Les DRS doivent fournir au bureau de l'équipe de [la solution de DSE] et aux DRS touchés un rapport d'incident lié à [la solution de DSE] dans les 72 heures suivant la demande du rapport.

1.20. Les versions définitives des rapports d'incident doivent être évaluées par le comité ConnexionSécurité et, au besoin, par l'organisme de surveillance compétent. Santé Ontario facilitera cet examen lorsque le rapport sera soumis par le DRS.

1.21. Les DRS devraient prévoir une méthode pour passer en revue leurs incidents liés à [la solution de DSE] au moins une fois par mois pour déterminer les tendances et chercher à savoir s'il est possible de prendre des mesures de prévention pour réduire les risques d'incidents similaires à l'avenir.

Collecte d'éléments de preuve

1.22. Les DRS devraient mettre en place des procédures pour recueillir des éléments de preuve dans le but d'intenter des poursuites judiciaires ou d'imposer des mesures disciplinaires contre les mandataires ou les fournisseurs de services électroniques. Ces procédures devraient exiger les éléments suivants :

1.22.1. la réalisation de travaux médico-légaux sur des copies des éléments de preuve;

1.22.2. le recours à un témoin lors de la création de copies;

1.22.3. la journalisation de l'information relative à la création des copies, notamment :

1.22.3.1. le moment et l'endroit où les activités de copie ont eu lieu;

1.22.3.2. la personne ayant effectué les activités de copie;

1.22.3.3. les outils ou programmes utilisés pour les activités de copie;

1.23. la protection de l'intégrité de tous les éléments de preuve.

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

2.1. L'équipe de [la solution de DSE] doit mettre en place un processus de gestion des incidents de sécurité de l'information (les « incidents ») qui traite de toutes les phases du processus de gestion des incidents :

- détection/triage;
- intervention;
- rétablissement;
- suivi.

2.2. Si, à tout moment au cours du processus de gestion des incidents, l'équipe de [la solution de DSE] se rend compte qu'il y a eu atteinte à la vie privée par suite de l'incident, ce dernier doit être traité conformément à la Politique de gestion des atteintes à la vie privée.

Détection/triage

2.3. L'équipe de [la solution de DSE] doit établir un point de contact à qui seront signalés les incidents qui ont lieu ou dont on soupçonne l'existence. Le plus souvent, c'est le soutien technique qui fait office de point de contact.

2.4. L'équipe de [la solution de DSE] doit veiller à ce que ses mandataires et ses fournisseurs de services électroniques sachent qu'ils doivent signaler sur-le-champ les incidents qui ont lieu ou dont on soupçonne l'existence.

2.5. Le point de contact doit créer un billet d'incident pour tout incident signalé. Il est recommandé d'utiliser un système de gestion automatisée des incidents pour consigner ces derniers. Le billet d'incident doit contenir les éléments suivants :

2.5.1. l'heure et la date de l'incident signalé;

2.5.2. le nom et les coordonnées du patient, du DRS, du mandataire ou du fournisseur de services électroniques qui a signalé l'incident;

2.5.3. l'information relative à l'incident signalé (type et mode de détection, par exemple);

2.5.4. toutes les conséquences de l'incident signalé;

2.5.5. toutes les mesures adoptées pour limiter l'incident soivent par le mandataire ou le fournisseur de services électroniques qui a signalé l'incident, soit par le point de contact.

2.6. L'équipe de [la solution de DSE] doit nommer un chef ou une équipe responsable d'effectuer les activités de triage, d'intervention, de rétablissement et de suivi de tous les incidents. Le chef ou l'équipe d'intervention peut être la même personne ou la même équipe faisant office de point de contact.

2.7. Le point de contact doit envoyer immédiatement tous les billets d'incident au chef ou à l'équipe d'intervention.

2.8. Le chef ou l'équipe d'intervention doit examiner le billet d'incident et toute l'information connexe pour déterminer s'il y a réellement eu incident.

2.9. Le chef ou l'équipe d'intervention doit classer tous les incidents qui ont réellement eu lieu en fonction de leur gravité (voir l'annexe A intitulée *Cotes de gravité et de priorité des incidents* pour toute l'information sur les cotes de gravité).

2.10. Le chef ou l'équipe d'intervention doit créer un rapport d'incident (voir l'annexe B intitulée *Contenu du rapport d'incident*).

2.11. Tous les rapports d'incident complets ou partiels doivent être traités au minimum conformément aux exigences de protection de l'information considérée comme confidentielle.

2.12. Si un incident qui provient d'un DRS touche plus d'un DRS ou [la solution de DSE], l'équipe de [la solution de DSE] peut diriger les activités de gestion des incidents.

2.13. L'équipe de [la solution de DSE] doit veiller à ce que son processus de gestion des incidents exige que le chef ou l'équipe d'intervention avise tout DRS touché ou Santé Ontario par courriel au plus tard à la fin du jour ouvrable suivant tout incident classé de niveau 1 ou 2 par l'équipe de [la solution de DSE].

L'avis doit contenir au minimum les éléments suivants :

2.13.1. l'heure et la date de l'incident signalé;

2.13.2. le nom et les coordonnées du mandataire et du fournisseur de services électroniques qui a signalé l'incident;

2.13.3. l'information relative à l'incident signalé (type et mode de détection, par exemple);

2.13.4. toutes les conséquences de l'incident signalé;

2.13.5. toutes les mesures adoptées pour limiter l'incident soivent par le mandataire ou le fournisseur de services électroniques qui a signalé l'incident, soit par le point de contact, soit par le chef ou l'équipe d'intervention.

2.14. L'équipe de [la solution de DSE] doit aviser Santé Ontario, qui avisera le comité ConnexionSécurité et l'organisme de surveillance compétent :

2.14.1. dans les 72 heures suivant l'avis pour tout incident de niveau de gravité 1;

2.14.2. dans la semaine suivant l'avis pour tout incident de niveau de gravité 2.

2.15. L'équipe de [la solution de DSE] doit établir la priorité de tous les incidents conformément à leur cote de gravité et de priorité.

Intervention

2.16. Le chef ou l'équipe d'intervention doit prendre les mesures nécessaires pour limiter la portée et l'ampleur d'un incident. Les activités d'atténuation ou de confinement peuvent être les suivantes :

2.16.1. effectuer une copie de sauvegarde du système d'information;

2.16.2. cesser les activités;

2.16.3. modifier les mots de passe ou les listes de contrôle d'accès du système d'information compromis;

2.16.4. restreindre la connexion.

NOTA : Selon la gravité de l'incident, il peut être nécessaire de mettre en œuvre les plans de continuité des activités de l'équipe de [la solution de DSE].

2.17. L'équipe de [la solution de DSE] devrait élaborer des stratégies de confinement pour chaque type d'incident majeur avec des critères clairs pour faciliter la prise de décisions. Les critères suivis pour élaborer ces stratégies peuvent être les suivants :

2.17.1. les risques de bris ou de vol de ressources;

2.17.2. la nécessité de conserver les éléments de preuve;

2.17.3. l'accessibilité des services (connectivité du réseau, services offerts à des parties externes);

2.17.4. le temps et les ressources nécessaires pour mettre les stratégies en œuvre;

2.17.5. l'efficacité des stratégies (confinement partiel ou intégral, par exemple);

2.17.6. la durée de la solution (solution de rechange en cas d'urgence à retirer dans quatre heures, solution de rechange temporaire à retirer dans deux semaines ou solution permanente, par exemple).

NOTA : Selon la gravité de l'incident et le type d'incident, il peut être nécessaire de mettre en œuvre les plans de continuité des activités de l'équipe de [la solution de DSE]. Des critères devraient donc être définis pour orienter le travail du chef ou de l'équipe d'intervention quant au moment où aviser le personnel responsable de la continuité des activités.

Rétablissement

2.18. L'équipe de [la solution de DSE] doit rétablir les systèmes d'information touchés de manière à ce qu'ils retrouvent un état de fonctionnement normal. Les activités de rétablissement peuvent être les suivantes :

2.18.1. éliminer la cause de l'incident (suppression d'un programme malveillant, par exemple);

2.18.2. restaurer les systèmes d'information et en valider l'état;

2.18.3. décider du moment de la reprise des activités;

2.18.4. surveiller les systèmes d'information pour voir s'ils fonctionnent bien et confirmer qu'il n'y a plus de données ou de systèmes compromis.

Suivi

2.19. L'équipe de [la solution de DSE] doit faire enquête à la suite de tous les incidents pour en déterminer la cause (par analyse par arbre de défaillances, par exemple).

2.20. Une fois un incident résolu (c'est-à-dire que toutes les activités de rétablissement ont été mises en œuvre et que les technologies de l'information et les systèmes d'information touchés sont revenus à leur état normal), le chef ou l'équipe d'intervention doit rédiger le rapport d'incident. Dans le cas des longues enquêtes, les DRS touchés doivent demander qu'on fasse le point sur l'enquête pendant le déroulement de cette dernière.

2.21. L'équipe de [la solution de DSE] doit archiver tous ses rapports d'incident pour au moins 24 mois.

2.22. L'équipe de [la solution de DSE] doit fournir au DRS participant tout rapport d'incident relatif à [la solution de DSE] dans les 72 heures suivant la demande.

2.23. Les versions définitives des rapports d'incident doivent être évaluées par le comité ConnexionSécurité et de sécurité et, au besoin, par l'organisme de surveillance compétent. Santé Ontario facilitera cet examen lorsque le rapport est soumis par le bureau de l'équipe de [la solution de DSE].

2.24. L'équipe de [la solution de DSE] doit prévoir une méthode pour passer en revue tous ses incidents au moins une fois par mois pour déterminer les tendances et chercher à savoir s'il est possible de prendre des mesures de prévention pour réduire les risques d'incidents similaires à l'avenir.

Collecte d'éléments de preuve

2.25. L'équipe de [la solution de DSE] devrait mettre en place des procédures pour recueillir des éléments de preuve dans le but d'intenter des poursuites judiciaires ou d'imposer des mesures disciplinaires contre les mandataires ou les fournisseurs de services électroniques. Ces procédures devraient exiger les éléments suivants :

2.25.1. la réalisation de travaux médico-légaux sur des copies des éléments de preuve;

2.25.2. le recours à un témoin lors de la création de copies;

2.25.3. la journalisation de l'information relative à la création des copies, notamment :

2.25.3.1. le moment et l'endroit où les activités de copie ont eu lieu;

2.25.3.2. la personne ayant effectué les activités de copie;

2.25.3.3. les outils ou programmes utilisés pour les activités de copie;

2.25.4. la protection de l'intégrité de tous les éléments de preuve.

Exceptions Toute exception à la norme doit être approuvée par l'organisme de surveillance compétent, lequel n'autorisera d'exceptions que 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 comptent.

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 le fournisseur de services électroniques ou la cessation des privilèges d'accès des mandataires, et de demander des mesures correctives.

Références

Lois

- LPRPS
- 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 et de normes sur les DSE de Santé Ontario

- Politique de sécurité de l'information
- Norme d'utilisation acceptable des données et des technologies de l'information
- Norme sur le contrôle de l'accès aux systèmes et les processus de gestion d'identité connexes
- Norme sur les fournisseurs d'identités fédérées et Manuel de procédures relatives à l'admissibilité
- Norme sur la continuité des activités
- Norme sur la cryptographie
- Norme sur les fournisseurs de services électroniques
- Norme sur la gestion des incidents de sécurité de l'information
- Norme sur la gestion de l'information et des éléments d'actif
- Norme sur les réseaux et les opérations
- Norme sur la journalisation de sécurité et la surveillance
- Norme sur le cycle de développement de systèmes
- Norme sur la sécurité matérielle
- Norme 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)

Annexe A : Cotes de gravité et de priorité des incidents

Cotes de gravité

Gravité	Catégorie et description	Durée maximale recommandée		
		Triage	**Confinement**	**Rétablissement**
1	**Critique** • Nombreux sites ou sites essentiels hors fonction • Perte de services qui entraîne des risques très importants pour les DRS participants • Constitue un risque en matière de santé publique, de protection des renseignements personnels ou de sécurité • A de graves répercussions sur bon nombre de systèmes internes ou externes, par exemple l'intrusion à grande échelle d'un programme malveillant Intervention et restauration immédiates : tout le monde met la main à la pâte	30 min	6 h	72 h
2	**Élevé** • Un seul site important hors de fonction • Perte d'un service non essentiel pour la mission de l'organisation • Soutien technique non accessible • Échec du rétablissement • Détérioration des services pour les DRS • Défaillance d'une application ou d'une composante qui affecte plusieurs clients Intervention et restauration le plus rapidement possible (dans le jour ouvrable)	2 h	12 h	24 h
3	**Moyen** • Ralentissement d'applications ou de composants matériels • Ennuis techniques mineurs • Panne d'une application ou d'un composant qui ne touche qu'un client Restauration au cours des prochains jours ouvrables	4 h	36 h	48 h
4	**Faible** • Répercussions minimales, aucun ralentissement ou présence d'une solution de rechange Restauration dans la semaine	24 h	36 h	15 jours

Cotes de priorité

Type d'incident	Cote de priorité	
	P2	P1
Contrôle de l'accès : Pour les incidents de sécurité relatifs à une mesure de contrôle de l'accès compromise.		
Compte avec privilèges compromis Par exemple, un identifiant avec privilèges (pour les administrateurs de système, les administrateurs de base de données ou les administrateurs de pare-feu) est associé à des activités inhabituelles (ouvertures de session inexpliquées ou accès étranges à des fichiers, par exemple).	X	
Détection d'une attaque par hameçonnage visant des utilisateurs avec privilèges Par exemple, de nombreux courriels suspects ciblant des utilisateurs ayant un accès avec privilèges.	X	
Sécurité des éléments d'actif : Pour les pertes ou les vols d'éléments d'actif et les attaques portées contre un élément d'actif entraînant une interruption de services.		
Perte de dispositifs de stockage non chiffrés Par exemple, la perte d'une clé USB non chiffrée contenant des données sensibles.	X	
Détection d'une attaque par déni de service contre un élément d'actif essentiel Par exemple, une attaque par déni de service a eu lieu contre un serveur hébergeant des applications essentielles.	X	
Sécurité des données : Pour les menaces à la confidentialité des données.		
Volume inhabituellement élevé de données à laquelle on a accès sur un serveur hébergeant des données sensibles ou des applications qui traitent ou stockent des données sensibles Par exemple, une alarme de système est déclenchée lorsqu'il y a un volume élevé de données transférées hors des heures d'ouverture (outre les sauvegardes de données).	X	
Détection d'une infection à un programme malveillant ou à un virus avec conséquences importantes Par exemple, une alarme est déclenchée lorsqu'il y a détection d'un virus.	X	
Intégrité des données et des systèmes : Pour les compromissions potentielles de l'intégrité de données et de systèmes.		
Atteinte majeure à la protection des données ayant attiré l'attention des médias Par exemple, une atteinte majeure à la protection des données ayant attiré l'attention des médias.		X
Panne de la sauvegarde sur bande pour une certaine période Par exemple, la sauvegarde sur bande n'a pas fonctionné pour les cinq dernières sessions.	X	

Annexe B : Contenu du rapport d'incident

Les éléments suivants sont obligatoires dans le rapport d'incident de sécurité de l'information :

1. Coordonnées du mandataire ou du fournisseur de services électroniques qui a signalé l'incident ET du chef ou de l'équipe d'intervention
    - Nom
    - Unité (service, division ou équipe, par exemple) (s'il y a lieu)
    - Courriel
    - Numéro de téléphone
    - Emplacement (adresse postale, immeuble et numéro de la porte, par exemple)
2. Information relative à l'incident
    - Date et heure auxquelles l'incident a été découvert
    - Date et heure estimées du début de l'incident
    - Numéro du billet d'incident
    - Type d'incident (refus de service, programme malveillant, accès non autorisé ou utilisation inappropriée, par exemple)
    - Emplacement physique de l'incident (ville, par exemple)
    - État actuel de l'incident (attaque répétée, par exemple)
    - Source/cause de l'incident (si elle est connue), y compris les noms d'hôte et les adresses IP
    - Description de l'incident (le mode de détection et ce qui s'est passé, par exemple)
    - Description des ressources touchées (réseaux, hôtes, applications ou données, par exemple), y compris les noms d'hôte, les adresses IP et la fonction des systèmes d'information
    - Système d'exploitation, version et dernier correctif apporté
    - Antivirus installé, activé et à jour (oui/non)
    - Facteurs d'atténuation
    - Estimation des répercussions techniques de l'incident (données supprimées, arrêt de fonctionnement du système ou application non accessible, par exemple)
    - Actions du mandataire ou du fournisseur de services électroniques qui a signalé l'incident (mise hors service de l'hôte ou déconnexion de l'hôte du réseau, par exemple)
    - Autres organisations jointes (fabricant du logiciel, par exemple)
    - Type d'information compromis (s'il y a lieu)
3. Commentaires généraux[1]
4. Résumé de l'incident
5. Coordonnées de toutes les parties concernées
6. Journal des actions de confinement ou d'atténuation de chef ou de l'équipe d'intervention

[1] Recommandés, mais non obligatoires.

7. Liste des éléments de preuve recueillis
8. Cause de l'incident (application mal configurée ou correctif non installé sur l'hôte, par exemple)
9. Liste des activités de rétablissement recommandées et mises en œuvre
10. État actuel de l'intervention