Ontario Health

Norme sur la continuité des activités

Version: 1.7

N° de document : 3536

`

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	2014-12-11
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	2013-12-20	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	2014-12-05	Révision en fonction des commentaires reçus des membres du Comité ConnexionSécurité. Ajout de la définition de « mandataire », de « terminal d'envoi de données » et de « service de gestion d'identité ». Ajout de l'obligation de valider les exigences opérationnelles au point 1.13; ajout des coordonnées et du plan de communication des intervenants qu'il faut joindre au point 1.10.9.	Mark Carter
1.2	2014-12-11	Révision à la suite de la réunion du Comité ConnexionSécurité du 11 décembre. Modification du point 2.12 de manière à indiquer que le plan de continuité des activités doit inclure au moins un des trois points mentionnés et que tous les scénarios doivent être mis à l'essai sur une période de trois ans. Approbation de la politique par les membres.	Mark Carter
1.3	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
1.4	2017-03-20	Mise à jour de la norme afin de refléter l'ITSM. Changement du titre du document, qui passe de	Raviteja Addepalli

`

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
		« Politique » à « Norme ». Mise à jour de la définition de « la solution de DSE ». Révision des contrôles en fonction des commentaires.	
1.5	March 16, 2018	Mise à jour de la norme afin d'inclure l'accès au DSE par les patients.	Geovanny Diaz
1.6	2020-04-27	Revision et mises à jour mineures faites dans le cadre de revision régulier établi par le Comité ConnexionSécurité..	Trina Dobson
1.7	2021-01-21	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 la continuité des activités

Objet

La présente norme a pour but de définir les exigences et les recommandations en vue de l'élaboration et de la mise en œuvre de plans de continuité des activités dans les buts suivants :

- faire en sorte que [la solution de DSE] demeure accessible ou puisse être restaurée en cas d'interruption;
- assurer le maintien de la transmission des renseignements personnels sur la santé (RPS) vers [la solution de DSE].

Portée

La présente norme s'applique à tous les services de [la solution de DSE], y compris la totalité des portails et des applications pour les patients.

Dans le cas des dépositaires de renseignements sur la santé (DRS) qui consultent, manipulent ou versent des RPS dans le dépôt de données cliniques de [la solution de DSE] ou assurent des services de gestion d'identité, la norme s'applique aussi aux éléments suivants :

- 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;
- 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 assurant 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.

Continuité des activités : Ensemble des activités visant à maintenir l'accès à [la solution de DSE] ou à gérer les interruptions d'accès. Inclut les éléments non techniques tels que les processus sur papier, les changements dans le déroulement des activités et l'allocation des ressources. Peut aussi inclure l'exécution d'un plan de rétablissement après catastrophe.

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.

Mandataire : Dans le contexte des dépositaires de renseignements sur la santé, personne qui, sous réserve de l'approbation du dépositaire, s'occupe de tout ce qui est lié aux renseignements personnels sur la santé de ce dernier, et ce, dans l'intérêt du dépositaire et non dans son propre intérêt, qu'il ait ou non le pouvoir d'engager le dépositaire, qu'il soit employé ou non par le dépositaire et qu'il soit rémunéré ou non. Par exemple, le mandataire peut être une organisation, un employé ou un entrepreneur qui valide l'identité des utilisateurs du dossier de santé électronique au nom d'un dépositaire de renseignements sur la santé. Un mandataire peut aussi assurer des services de correction de données d'un dépositaire de renseignements sur la santé à partir de son terminal d'envoi de données.

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.

`

Rétablissement après catastrophe : Ensemble des activités déterminant les mesures nécessaires pour rétablir les systèmes d'information permettant d'accéder à [la solution de DSE].

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

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

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

Terminal d'envoi de données : Technologies et processus connexes qui alimentent le dépôt de données cliniques et font l'objet des recherches de données par l'utilisateur en milieu clinique. Comprend habituellement le système d'information (système d'information hospitalier, système d'information de laboratoire, système d'information clinique, 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 veiller à ce que les exigences des services de gestion d'identité et des terminaux d'envoi de données liés à [la solution de DSE] soient intégrées à leur stratégie de continuité des activités et devraient faire ce qui suit :

1.1.1. mettre en place une infrastructure technique résiliente avec des plans de rétablissement après catastrophe;

1.1.2. coordonner et conserver des plans de continuité des activités et les dispositions à cet effet;

1.1.3. valider les plans de continuité des activités de manière à ce que les exigences soient respectées.

1.2. Les DRS devraient veiller à ce qu'on cerne, dans la stratégie de continuité des activités, les services de gestion d'identité et les terminaux d'envoi de données visés par les plans de continuité des activités et les dispositions à cet effet et qu'on consigne l'information pertinente (dans un registre des risques à la continuité des activités, par exemple) concernant les points suivants :

1.2.1. les activités visées par les plans;

1.2.2. les principaux intervenants à l'interne et à l'externe.

Résilience

1.3. Les DRS devraient prévoir des méthodes pour réduire les risques de mauvais fonctionnement de leurs services de gestion d'identité et de leurs terminaux d'envoi de données parmi les suivantes :

1.3.1. employer des marques ou modèles à jour de pièces informatiques et de logiciels dont il est facile de faire l'entretien ou la maintenance et qui sont capables d'assurer les processus essentiels;

1.3.2. accorder la priorité à la fiabilité, à la compatibilité et à la capacité dans le processus d'acquisition;

1.3.3. assurer le respect des normes générales ou de l'industrie pour le matériel et les logiciels;

1.3.4. utiliser des liaisons de réseau et des services de télécommunications résistants et résilients.

1.4. Les DRS devraient prévoir des méthodes pour veiller à ce que leurs services de gestion d'identité et leurs terminaux d'envoi de données demeurent accessibles parmi les suivantes :

1.4.1. faire fonctionner les systèmes d'information essentiels en même temps à divers endroits (à l'aide d'une technologie de secours immédiat ou de virtualisation);

1.4.2. trouver d'autres emplacements à partir desquels les systèmes d'information peuvent être exécutés et administrés;

`

1.4.3. déterminer automatiquement les opérations touchées et en assurer le rétablissement en cas de panne des systèmes d'information.

1.5. Les DRS devraient réduire les points de défaillance dans leur réseau par l'un ou l'autre des moyens suivants :

1.5.1. rediriger la circulation sur le réseau automatiquement lorsque de l'équipement ou des liaisons tombent en panne;

1.5.2. installer des composants en double ou de remplacement (éléments d'actif, plateformes, ponts, concentrateurs, commutateurs, pare-feu et filtres de trafic sur le réseau, par exemple) pour l'équipement essentiel;

1.5.3. prévoir d'autres points de connexion et de liaison avec des fournisseurs de services externes.

1.6. Les DRS devraient élaborer une méthode pour gérer les défaillances de leurs services de gestion d'identité et de leurs terminaux d'envoi de données, méthode qui peut inclure les étapes suivantes :

1.6.1. enregistrer toutes les défaillances réelles ou présumées;

1.6.2. aviser les personnes touchées par les défaillances dans des délais raisonnables;

1.6.3. désactiver les systèmes et les services dans lesquels on soupçonne des défaillances jusqu'à ce qu'on remédie à la situation;

1.6.4. veiller à ce qu'on répare ou remplace les éléments touchés selon les délais à respecter.

Planification

1.7. Les DRS devraient posséder un plan de continuité des activités pour chacun de leurs services de gestion d'identité et de leurs terminaux d'envoi de données dans le cadre de leur stratégie de continuité des activités pour participer à [la solution de DSE].

1.8. Les DRS devraient nommer un propriétaire des services de gestion d'identité et des terminaux d'envoi de données (ou un groupe de services de gestion d'identité et de terminaux d'envoi de données), lequel sera responsable d'élaborer, de mettre à l'essai et de mettre en œuvre les plans de continuité des activités et les dispositions à cet effet pour ses services de gestion d'identité et ses terminaux d'envoi de données.

1.9. Les DRS devraient établir leur plan de continuité des activités en fonction des résultats d'une évaluation des risques, laquelle peut comprendre les étapes suivantes :

1.9.1. évaluer les effets potentiels associés à l'interruption de systèmes d'information essentiels;

1.9.2. évaluer les risques d'interruption des systèmes d'information essentiels en effectuant une évaluation des menaces et des risques d'après un ensemble de scénarios catastrophes plausibles;

1.9.3. obtenir l'autorisation de la haute direction concernant les plans de continuité des activités et les dispositions à cet effet à adopter pour traiter les risques relevés.

`

1.10. Le plan de continuité des activités d'un DRS concernant ses services de gestion d'identité et ses terminaux d'envoi de données devrait inclure les éléments suivants :

1.10.1. les conditions entraînant son utilisation;

1.10.2. la marche à suivre pour entreposer en toute sécurité le plan (à l'extérieur du site, par exemple) et les récupérer en cas d'urgence;

1.10.3. la période maximale d'interruption permise, soit la durée totale d'une interruption des systèmes d'information que peut soutenir une organisation;

1.10.4. le déroulement des activités de rétablissement à effectuer, y compris les procédures de transition vers d'autres réseaux en cas d'urgence et les procédures de reprise (en ordre de priorité);

1.10.5. les rôles et responsabilités des personnes chargées d'effectuer chaque activité;

1.10.6. les mesures de contrôle de sécurité de l'information à appliquer après la mise en œuvre du plan de continuité des activités (protéger la confidentialité et l'intégrité des renseignements personnels sur la santé [RPS], par exemple);

1.10.7. les tâches à accomplir après rétablissement et restauration (par exemple, vérifier si les systèmes et les renseignements sont dans le même état qu'ils étaient avant la mise en œuvre du plan de continuité des activités);

1.10.8. le propriétaire du plan et une note sur la plus récente évaluation du bien-fondé du plan;

1.10.9. les coordonnées et le plan de communication des intervenants et des responsables qu'il faut joindre.

Testing

1.11. Les DRS devraient passer en revue et mettre à l'essai leurs plans de continuité des activités pour leurs services de gestion d'identité et leurs terminaux d'envoi de données chaque année, ce qui peut inclure l'un ou l'autre des éléments suivants :

1.11.1. des essais simples par lesquels on effectue une révision structurée sous forme de répétitions entre les intervenants selon divers scénarios d'application du plan de continuité des activités;

1.11.2. des essais de niveau intermédiaire par lesquels on effectue des simulations du plan de continuité des activités selon divers scénarios et des essais parallèles dans le cadre desquels on fait appel aux installations de rechange pour éviter l'interruption des systèmes d'information;

1.11.3. des essais complexes par lesquels on simule une interruption complète de l'activité du site principal pour tester le fonctionnement des installations de rechange dans son intégralité.

1.12. Les DRS devraient conserver un registre des essais réalisés contenant la date, les résultats et l'autorisation de l'une des personnes de la haute direction (le dirigeant principal de l'information, par exemple).

`

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

2.1. L'équipe de [la solution de DSE] doit veiller à ce que les exigences en matière de protection de l'information et de technologies de l'information soient intégrées à sa stratégie de continuité des activités et faire ce qui suit :

2.1.1. mettre en place une infrastructure technique résiliente avec des plans de rétablissement après catastrophe;

2.1.2. coordonner et conserver des plans de continuité des activités et les dispositions à cet effet;

2.1.3. valider les plans de continuité des activités de manière à ce que les exigences soient respectées.

2.2. L'équipe de [la solution de DSE] doit veiller à ce qu'on cerne, dans la stratégie de continuité des activités, les systèmes d'information visés par les plans de continuité des activités et les dispositions à cet effet et qu'on consigne l'information pertinente (dans un registre des risques à la continuité des activités, par exemple) concernant les points suivants :

2.2.1. les systèmes d'information essentiels (en ordre de priorité) et les processus qu'ils prennent en charge;

2.2.2. les principaux intervenants à l'interne et à l'externe.

Résilience

2.3. L'équipe de [la solution de DSE] devrait veiller à ce que [la solution de DSE] soit résistante, fiable et prise en charge par des installations de remplacement ou en double.

2.4. L'équipe de [la solution de DSE] doit mettre en œuvre des méthodes pour réduire les risques de mauvais fonctionnement des systèmes d'information parmi lesquelles doivent être incluses les suivantes :

2.4.1. employer des marques ou modèles à jour de pièces informatiques et de logiciels dont il est facile de faire l'entretien ou la maintenance et qui sont capables d'assurer les processus essentiels;

2.4.2. accorder la priorité à la fiabilité, à la compatibilité et à la capacité dans le processus d'acquisition;

2.4.3. assurer le respect des normes générales ou de l'industrie pour le matériel et les logiciels;

2.4.4. utiliser des liaisons de réseau et des services de télécommunications résistants et résilients.

2.5. L'équipe de [la solution de DSE] doit mettre en œuvre des méthodes pour veiller à ce que les systèmes d'information demeurent accessibles parmi les suivantes :

2.5.1. faire fonctionner les systèmes d'information essentiels en même temps à divers endroits (à l'aide d'une technologie de secours immédiat ou de virtualisation);Providing alternative locations from which information systems can be run and administered.

`

2.5.2. trouver d'autres emplacements à partir desquels les systèmes d'information peuvent être exécutés et administrés;

2.5.3. déterminer automatiquement les opérations touchées et en assurer le rétablissement en cas de panne des systèmes d'information.

2.6. L'équipe de [la solution de DSE] doit réduire les points de défaillance dans son réseau par l'un ou l'autre des moyens suivants :

2.6.1. rediriger la circulation sur le réseau automatiquement lorsque de l'équipement ou des liaisons tombent en panne;

2.6.2. installer des composants en double ou de remplacement (éléments d'actif, plateformes, ponts, concentrateurs, commutateurs, pare-feu et filtres de trafic sur le réseau, par exemple) pour l'équipement essentiel;

2.6.3. prévoir d'autres points de connexion et de liaison avec des fournisseurs de services externes.

2.7. L'équipe de [la solution de DSE] devrait élaborer une méthode pour gérer les défaillances, laquelle peut comprendre les étapes suivantes :

2.7.1. enregistrer toutes les défaillances réelles ou présumées;

2.7.2. aviser les personnes touchées par les défaillances dans des délais raisonnables;

2.7.3. désactiver les systèmes d'information et les services dans lesquels on soupçonne des défaillances jusqu'à ce qu'on remédie à la situation;

2.7.4. veiller à ce qu'on répare ou remplace les systèmes d'information essentiels selon les délais à respecter.

Planification

2.8. L'équipe de [la solution de DSE] doit veiller à ce qu'on rédige un plan de continuité des activités pour chaque système d'information (ou groupe de systèmes d'information connexes) dans le cadre de sa stratégie de continuité des activités.

2.9. L'équipe de [la solution de DSE] doit nommer un propriétaire pour chaque système d'information (ou groupe de systèmes d'information connexes), lequel sera responsable d'élaborer, de mettre à l'essai et de mettre en œuvre les plans de continuité des activités et les dispositions à cet effet pour ses systèmes d'information.

2.10. L'équipe de [la solution de DSE] doit établir le plan de continuité des activités en fonction des résultats d'une évaluation des risques, laquelle doit comprendre les étapes suivantes :

2.10.1. évaluer les effets potentiels associés à l'interruption de systèmes d'information essentiels;

2.10.2. évaluer les risques d'interruption des systèmes d'information essentiels d'après un ensemble de scénarios catastrophes plausibles;

`

2.10.3. obtenir l'autorisation d'un membre de la haute direction (le dirigeant principal de l'information, par exemple) concernant les plans de continuité des activités et les dispositions à cet effet à adopter pour traiter les risques relevés.

2.11. Le plan de continuité des activités de chaque système d'information essentiel (ou groupe de systèmes d'information connexes) doit inclure les éléments suivants :

2.11.1. les conditions entraînant son utilisation;

2.11.2. la marche à suivre pour entreposer en toute sécurité le plan (à l'extérieur du site, par exemple) et les récupérer en cas d'urgence;

2.11.3. la période maximale d'interruption permise, soit la durée totale d'une interruption des systèmes d'information que peut soutenir une organisation;

2.11.4. le déroulement des activités de rétablissement à effectuer, y compris les procédures de transition vers d'autres réseaux en cas d'urgence et les procédures de reprise (en ordre de priorité);

2.11.5. les rôles et responsabilités des personnes chargées d'effectuer chaque activité;

2.11.6. les mesures de contrôle de sécurité de l'information à appliquer après la mise en œuvre du plan de continuité des activités (protéger la confidentialité et l'intégrité des renseignements, par exemple);

2.11.7. les tâches à accomplir après rétablissement et restauration (par exemple vérifier si les systèmes et les renseignements sont dans le même état qu'ils étaient avant la mise en œuvre du plan de continuité des activités);

2.11.8. le propriétaire du plan et une note sur la plus récente évaluation du bien-fondé du plan;

2.11.9. les coordonnées et le plan de communication des intervenants et des responsables qu'il faut joindre.

Mise à l'essai

2.12. At a minimum, [the EHR Solution] Program must review and test their business continuity plans annually, which must include at least one of the following, with each scenario being tested within a period of three years:

2.12.1. Simple tests, which involve structured walk-through tests where stakeholders meet to rehearse the business continuity plan using different scenarios.

2.12.2. Medium tests, which involve simulation tests where staff test the business continuity plan using specific scenarios and parallel tests where alternative facilities are used to avoid disrupting production information systems.

2.12.3. Complex tests, which involve full-interruption tests where the original site is shut down and a complete test is performed at an alternative facility.

`

2.13. [The EHR Solution] Program must maintain a record of the execution of the tests with the date, the results, and sign-off from a senior-level executive (e.g., CIO).

Dérogations Toute exception 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.

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.

References

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 et de normes sur les DSE de Santé Ontario

- ISO/IEC 27001:2013, Information Technology – Security Techniques – Information Security Management Systems – Requirements
- ISO/IEC 27002:2013, Information Technology – Security Techniques – Code of Practice for Information Security Management
- ISO/IEC 27005: 2018 Information Technology – Security Techniques – Information Security Risk Management
- ISO 27799:2016 Health Informatics – Information security management in health using ISO/IEC 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)