CANADIAN PARTNERSHIP AGAINST CANCER

PARTENARIAT CANADIEN CONTRE LE CANCER

Manuel des normes de la Politique de cybersécurité

En vigueur à partir du 15 janvier 2020

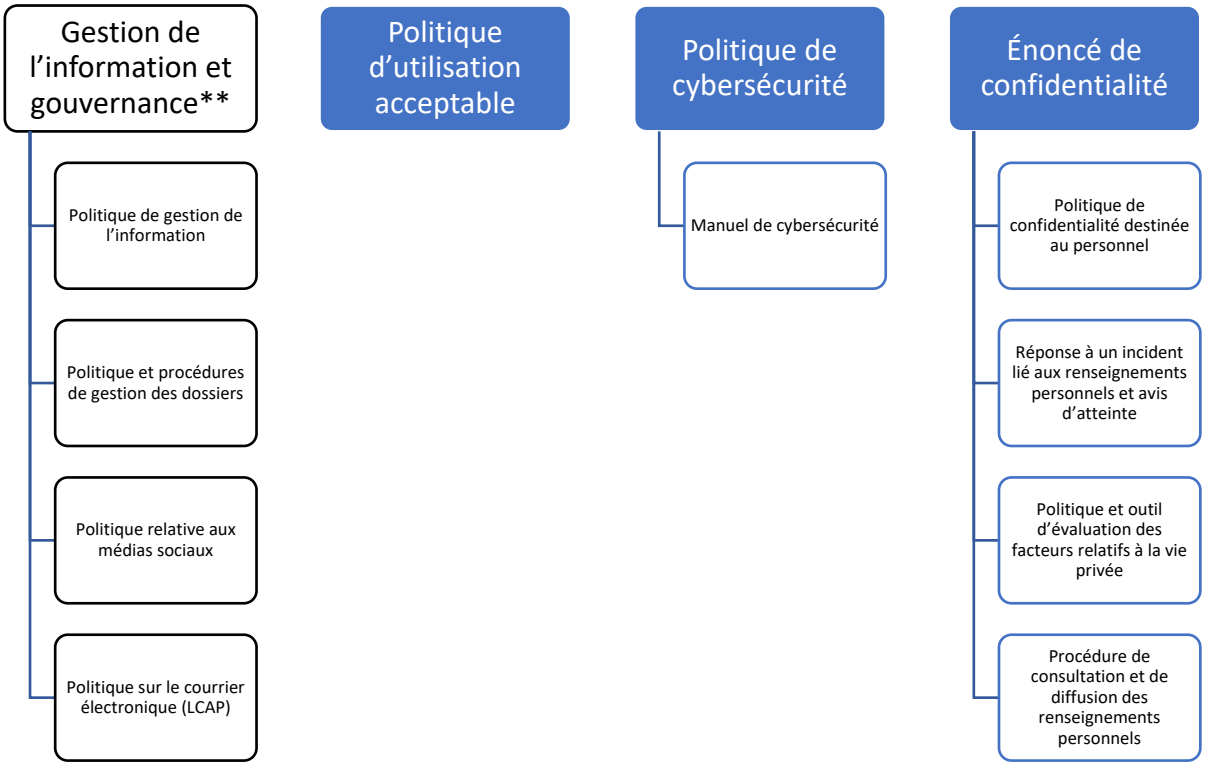
Table des matières

OBJET

Le présent manuel décrit et répertorie les normes et les processus en matière de cybersécurité pour les systèmes de TI, les réseaux et les solutions en nuage partagés, et sert de référence de base pour le Partenariat.

On y trouve **les normes, les procédures et les processus** qui décrivent le programme de cybersécurité.

Il décrit les processus où le Partenariat canadien contre le cancer (le Partenariat) travaille en collaboration avec les responsables d'information, les chefs de service et les intervenants du Partenariat pour établir des processus de sécurité efficaces et intégrés.



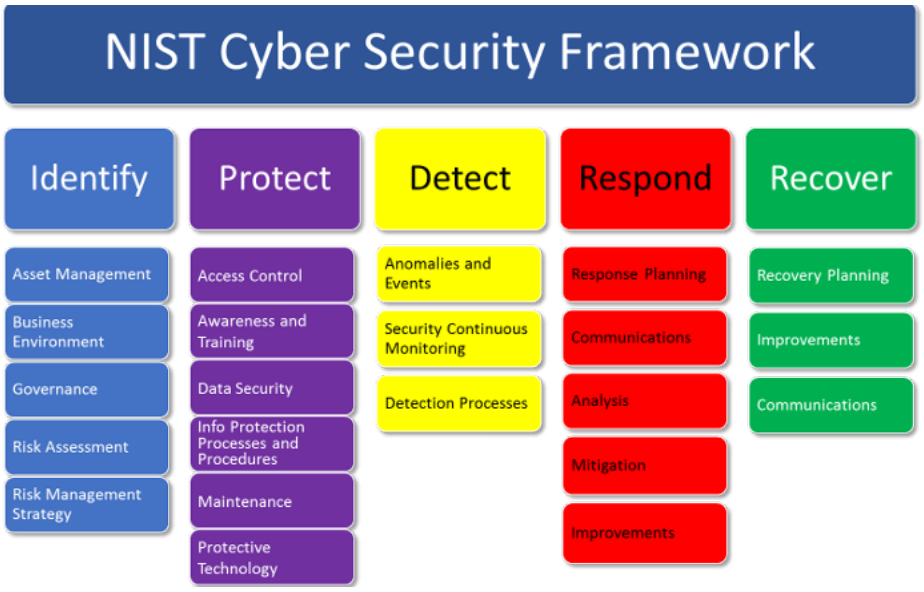
** Les politiques de gestion de l'information et de gouvernance ne font pas partie du Manuel de cybersécurité.

Introduction

Le manuel des normes liées aux politiques de cybersécurité du Partenariat a été élaboré à partir du cadre de cybersécurité de l'Institut national des normes et des technologies. Ce cadre est le guide du gouvernement des États-Unis destiné aux organisations du secteur privé qui possèdent, exploitent ou fournissent des infrastructures essentielles, et donne de l'information de base concernant la cybersécurité. Le cadre établit les processus et les contrôles de base pour la cybersécurité selon les cinq domaines suivants :

1. Identifier
2. Protéger
3. Détecter
4. Répondre
5. Récupérer

Le diagramme ci-dessous illustre les fonctions et les catégories qui composent le contenu principal du cadre :



Pour en savoir plus sur les directives et les sources qui ont été utilisées dans la préparation de ce manuel des normes de cybersécurité, veuillez consulter les ressources suivantes :

- **Organisation internationale de normalisation (ISO):27001** – Systèmes de management de la sécurité de l'information[1]
- **ISO: 27002** – Code de bonne pratique pour le management de la sécurité de l'information[2]
- **SANS Institute**[3]
- **Lignes directrices ITSG-33 du gouvernement du Canada**[4]

1. IDENTIFICATION DES RISQUES

1.1 Processus de gestion des risques

Le Partenariat établira un processus de gestion des risques pour la sécurité des TI, comme démontré à l'*annexe B*. Ce processus servira à évaluer les risques et à constituer le registre des risques liés aux TI.

1.2 Norme d'évaluation des risques et de certification des systèmes

Une norme d'évaluation des risques servira à évaluer efficacement les risques en matière de cybersécurité, en fonction des biens, des vulnérabilités et du contexte des menaces.

La certification des systèmes sert à vérifier si les exigences de sécurité établies pour un système ou un service en particulier sont respectées et si les contrôles et les mesures de protection fonctionnent comme prévu. Elle confirme que la direction a autorisé le fonctionnement du système ou l'exploitation du service en question et qu'elle a accepté le risque résiduel connexe. Le type de certification dépend de la quantité et de la qualité des éléments probants de certification exigés par l'organisme délivrant la certification.

Ces éléments probants peuvent inclure les résultats de toute évaluation des menaces et des risques, évaluation des répercussions sur les activités, évaluation des répercussions sur la protection des renseignements personnels, évaluation de la vulnérabilité, évaluation des essais et des produits de sécurité, autoévaluations, vérifications et examens de sécurité, ainsi que les

[1] ISO:27001 – https://www.iso.org/fr/standard/54534.html
[2] ISO: 27002 – https://www.iso.org/fr/standard/54533.html
[3] SANS Institute – https://www.sans.org
[4] ITSG-33 – https://cyber.gc.ca/fr/orientation/la-gestion-des-risques-lies-la-securite-des-ti-une-methode-axee-sur-le-cycle-de-vie

résultats des évaluations juridiques ou stratégiques connexes apportant la preuve de la conformité aux lois ou politiques pertinentes. En conséquence :

1.2.1 Les évaluations des risques à la sécurité des TI serviront à tenir compte des changements au contexte des menaces et au milieu technologique en général. L'équipe des TI peut également déterminer qu'une évaluation des risques est nécessaire pendant un changement, une mise à niveau ou un examen systématique des systèmes d'information. L'évaluation des risques se fera selon le processus de gestion des risques de l'équipe des TI qui figure à l'*annexe B*.

1.2.2 Des évaluations des facteurs relatifs à la vie privée seront menées pour les ressources informationnelles et de TI du Partenariat chaque fois qu'on apporte des changements qui pourraient influer sur la protection des renseignements personnels de ces ressources.

1.2.3 Le Partenariat examinera périodiquement les risques menaçant les systèmes ou les services en cas de modifications importantes ou lorsque cela s'avèrera nécessaire à la suite de changements survenus dans l'environnement de risque.

1.3 Norme des mesures de risques de cybersécurité et d'établissement de rapports

Afin de veiller à ce que les cybermenaces organisationnelles soient recensées, surveillées et corrigées, un registre des risques détaillés est nécessaire aux opérations de cybersécurité du Partenariat.

1.3.1 L'équipe des TI produira un registre des risques liés aux TI. Les mesures fourniront un résumé des risques, des vulnérabilités, des mesures correctives et des indicateurs clés quant aux risques et au rendement en matière de cybersécurité.

1.3.2 L'équipe des TI rendra compte des risques en matière de cybersécurité au directeur des technologies de l'information de façon régulière et au besoin, pour le renvoi des risques à un niveau supérieur, le soutien à la correction ou la conformité.

1.4 Norme de classification des données

La **norme de classification des données** s'applique à toutes les données, quel que soit l'environnement dans lequel elles se trouvent. Les données doivent être gérées de manière exacte, fiable et sécurisée, et être facilement accessibles pour un usage autorisé. Les mesures de sécurité des données seront mises en œuvre en fonction de la valeur, de la sensibilité et du risque des données. Les données sont classées en plusieurs catégories afin de réduire les normes et les contrôles contradictoires, d'établir des lignes directrices pour la conformité aux lois et règlements et de mettre en place des contrôles de sécurité de niveau pertinent.

1.4.1 Il incombera à l'ensemble du personnel, des consultants et des sous-traitants du Partenariat manipulant des renseignements administrés par le Partenariat ou qui sont sous son contrôle de comprendre et d'appliquer cette norme.

1.4.2 Il incombera à l'ensemble du personnel, des consultants et des sous-traitants du Partenariat mettant en œuvre des contrôles sur ses systèmes de TI en matière de sécurité et de protection des renseignements personnels de veiller à ce que lesdits contrôles soient appropriés et proportionnels au degré de sensibilité des renseignements gérés.

1.4.3 Tous les renseignements classifiés comme internes, confidentiels ou à diffusion restreinte devront faire l'objet de contrôles suffisants en matière de sécurité et de protection des renseignements personnels afin que l'accès à ces renseignements soit réservé aux utilisateurs autorisés.

1.4.4 Les données devront être recensées, « étiquetées » lorsqu'il y a lieu et manipulées en conformité avec le tableau de classification ci-dessous.

Classification	Description	Information Exemples de ressources	Incidence du risque	Exigences en matière de sécurité d'accès
Public	Renseignements accessibles au grand public, aux partenaires et au personnel	• Contenu du site Web • Rapports publiés • Matériels promotionnels • Offres d'emploi • Présentations externes	• Aucune répercussion • Inconvénient minimal en cas de non-disponibilité	Aucune

Classification	Description	Information Exemples de ressources	Incidence du risque	Exigences en matière de sécurité d'accès
Interne	Renseignements accessibles au personnel et aux personnes autorisées ne faisant pas partie du personnel (consultants et sous-traitants) ayant un « besoin de savoir » pour des motifs professionnels	• Documents de planification • Rapports d'avancement de projets • Ordre du jour et procès-verbal de réunions • Documents contenant des coordonnées professionnelles • Documents de planification stratégique • Documents opérationnels • Politiques et procédures • Conseils d'orientation stratégique	• Perturbation des activités en cas de non-disponibilité • Faible degré de risque en cas de corruption ou de modification	- Nécessité d'une authentification améliorée à un facteur pour l'accès des utilisateurs au réseau du Partenariat et d'un système de gestion des dossiers
Confidentiel	Renseignements exclusivement accessibles aux personnes appartenant à un groupe particulier ou occupant une fonction ou un poste précis	• Fichiers du personnel • Renseignements bancaires de personnes ne faisant pas partie du personnel du Partenariat • Contrats • Rapports financiers	• Atteinte à la réputation ou perte d'un avantage concurrentiel • Perte de confiance dans le Partenariat • Atteinte à la vie privée	- Contrôle d'accès au niveau du dossier uniquement pour les utilisateurs autorisés - Le chiffrement est conseillé pour le réseau

Classification	Description	Information Exemples de ressources	Incidence du risque	Exigences en matière de sécurité d'accès
		• Délibérations et documents complémentaires du comité de direction du conseil d'administration • Autres comités du conseil d'administration • Renseignements des partenaires désignés comme étant de nature délicate • Renseignements commerciaux de tiers transmis avec la mention « Confidentiel » • Renseignements sur les rémunérations • Conseils juridiques • Fichiers de signatures électroniques • Demandes de propositions et demandes de financement non attribuées • Enregistrements audio de réunions	• Atteinte à la propriété intellectuelle • Occasion manquée • Perte financière • Degré élevé de risque en cas de corruption ou de modification • Compromission des délibérations du conseil d'administration • Violation de la vie privée • Destruction de partenariats et de relations	de l'organisation. - Le chiffrement est nécessaire pour les réseaux externes et le stockage.

Classification	Description	Information Exemples de ressources	Incidence du risque	Exigences en matière de sécurité d'accès
À diffusion restreinte	Renseignements exclusivement accessibles à des personnes désignées ou aux titulaires de certains postes	• Casiers et enquêtes judiciaires • Dossiers de procédure • Bases de données comme le registre du cancer, exclusivement accessibles aux personnes désignées • Renseignements personnels sur la santé tels qu'ils sont décrits dans la *Loi sur la protection des renseignements personnels sur la santé de l'Ontario* (LPRPS)	• Blessure grave • Atteinte à la sécurité publique • Importantes pertes financières • Conséquences juridiques notables • Dommages importants	- Authentification de l'utilisateur à deux facteurs requise - Des journaux de vérification sont requis. - Les données doivent être chiffrées ou stockées dans des environnements sécurisés et approuvés par le directeur de la sécurité de l'information. - Les gestionnaires de service doivent examiner périodiquement l'accès et les contrôles.

2. PROTECTION DE L'INFORMATION

2.1 Norme d'authentification des utilisateurs et des contrôles d'accès

La **norme d'authentification des utilisateurs et des contrôles d'accès** garantit que seuls les utilisateurs autorisés peuvent accéder aux systèmes et à l'information du Partenariat. Les contrôles d'accès gèrent l'accès des utilisateurs à ces ressources, selon les besoins. Le Partenariat permet l'accès à ses systèmes et à ses données en fonction du principe du besoin de savoir et du principe de droit d'accès minimal.

Gestion des comptes

2.1.1 Un gestionnaire ou un responsable hiérarchique supérieur doit être désigné pour chacun des comptes du système.
2.1.2 Les comptes administratifs, partagés et de service doivent être approuvés par le directeur des technologies de l'information.
2.1.3 Les comptes privilégiés doivent être propres aux individus, et non génériques, et être approuvés par le directeur des technologies de l'information et du chef de service dont relève l'utilisateur.
2.1.4 Tous les comptes doivent être supprimés ou désactivés immédiatement en cas de cessation d'emploi, de démission ou d'achèvement de contrat. Cela doit faire partie des processus des ressources humaines et de l'approvisionnement, et être consigné dans le système de billetterie.
2.1.5 Les comptes de système d'employés engagés dans un processus de congé autorisé doivent être désactivés dans le cadre du processus des ressources humaines.
2.1.6 Les comptes utilisateur seront désactivés après 90 jours d'inactivité.
2.1.7 Les demandes d'accès ou de comptes utilisateur doivent être consignées et approuvées par l'équipe des TI par le biais d'un système de billetterie.
2.1.8 Les comptes utilisateur temporaires seront configurés pour expirer automatiquement à une date prédéfinie ou à la date d'échéance du contrat.
2.1.9 Les comptes utilisateur existants et leurs droits d'accès seront revus et approuvés tous les trimestres par les superviseurs des employés pour repérer les comptes qui ne sont plus utilisés, ou les comptes ayant des privilèges non requis.

2.1.10 Les comptes partagés et leurs droits d'accès seront revus et approuvés tous les trimestres par le directeur des technologies de l'information.

2.1.11 Les comptes sous-traitant et fournisseur sont octroyés après la signature d'une entente de confidentialité et doivent être approuvés par le directeur des technologies de l'information.

Contrôle des accès

2.1.12 Tous les comptes utilisateur doivent avoir un identificateur unique.

2.1.13 L'authentification à deux facteurs est requise pour l'accès aux systèmes à distance, ainsi que pour les systèmes essentiels et les administrateurs.

2.1.14 Les sessions d'utilisateur et les sessions du système doivent se verrouiller automatiquement après un maximum de 15 minutes d'inactivité.

2.1.15 Toutes les ouvertures de session ainsi que les tentatives infructueuses d'ouverture de session des utilisateurs doivent être enregistrées et stockées pendant un an. Ensuite, les données peuvent être détruites de façon sécurisée ou transférées à un support de stockage à long terme ou à un support d'archivage numérique.

Gestion des mots de passe

2.1.16 Tous les mots de passe dotés de privilèges de niveau « système » (super-utilisateurs, activation, administrateurs, comptes d'administration d'application, etc.) doivent être modifiés au moins une fois par année par l'équipe des TI.

2.1.17 Tous les mots de passe utilisateur (courriels, sites Web, ordinateurs de bureau, etc.) doivent être modifiés tous les 90 jours.

2.1.18 Les comptes seront temporairement bloqués pendant 15 minutes après trois tentatives infructueuses d'ouverture de session, et verrouillés après 10 tentatives. Cela devrait comprendre une notification aux administrateurs du système aux fins de vérification.

2.1.19 Les mots de passe récents ne doivent pas être réutilisés; l'historique des mots de passe doit donc conserver en mémoire ces mots de passe et empêcher les utilisateurs de les choisir de nouveau.

2.1.20 Les mots de passe ne doivent pas être :

i. Insérés dans des courriels ou dans d'autres types de communication électronique

ii. Imprimés sur papier
iii. Écrits sur des *Post-it* ou au dos de livres
iv. Stockés dans des fichiers de texte en clair (texte non chiffré)
v. Dans le cas où une de ces règles serait enfreinte, il faut agir comme s'il y avait eu un incident et changer immédiatement les mots de passe concernés.

2.1.21 Les mots de passe de production doivent être différents des mots de passe de non-production.

2.1.22 Toute divulgation soupçonnée d'un mot de passe ou toute activité suspecte en relation avec un compte doit être signalée à l'équipe des TI.

2.2 Norme de sécurité des réseaux sans fil

2.2.1 Le Partenariat doit isoler les réseaux sans fil de l'organisation des réseaux sans fil destinés aux invités.

2.2.2 Tous les réseaux sans fil gérés par le Partenariat seront administrés efficacement (p. ex. filtrage de contenu Web, pare-feu, prévention d'intrusion et capacités d'ouverture de session).

2.2.3 Le réseau sans fil des invités du Partenariat doit être protégé par un mot de passe modifié tous les mois.

2.2.4 Les employés du Partenariat ne doivent communiquer le mot de passe du réseau sans fil des invités qu'à des personnes de confiance.

2.2.5 Le Partenariat ne doit pas diffuser le SSID du réseau de l'organisation.

2.3 Norme de sécurité du réseau VPN du Partenariat

L'accès à distance par réseau VPN aux services de technologie de l'information en nuage ou locaux du Partenariat doit être géré et sécurisé efficacement.

2.3.1 Il faut utiliser des solutions commerciales de la génération actuelle ayant des algorithmes cryptographiques robustes, approuvés par le gouvernement du Canada.

2.3.2 Le Partenariat doit appliquer de solides processus d'authentification pour la connexion à distance par réseau VPN.

2.3.3 Les solutions et appareils du Partenariat doivent être approuvés par le directeur des technologies de l'information.

2.3.4 Les correctifs de système d'exploitation les plus récents, ainsi que les correctifs les plus récents des solutions de sécurité des points terminaux et contre les logiciels malveillants, doivent être installés et tenus à jour sur tous les appareils se connectant au réseau du Partenariat à distance.

2.3.5 Les demandes d'accès aux comptes doivent être approuvées par l'équipe des TI et le superviseur de l'employé ou du sous-traitant.

2.3.6 L'accès à distance doit être désactivé dès que l'employé du Partenariat, le sous-traitant ou le tiers n'en a plus besoin.

2.3.7 Le Partenariat se réserve le droit d'examiner par voie électronique tous les appareils qui se connectent à son réseau avant d'y fournir un accès à distance.

2.3.8 Tous les trimestres, les superviseurs réévalueront si les employés de leur service ont besoin de se connecter au Partenariat à distance au moyen d'un accès VPN.

2.3.9 Les utilisateurs approuvés pour l'accès à distance ne permettront pas l'accès non autorisé à d'autres personnes, y compris les membres de leur famille.

2.4 Norme de protection des points terminaux et des appareils mobiles (y compris les appareils personnels)

La **norme de protection des points terminaux et des appareils mobiles** garantit la bonne configuration des appareils. Notamment, on s'assure d'effectuer les mises à jour du système d'exploitation et des applications, et on met en place des mécanismes de contrôle d'accès et des restrictions d'accès. L'intégrité, la confidentialité et la disponibilité des données doivent être maintenues en tout temps. L'utilisation d'appareils mobiles personnels et d'appareils mobiles de l'organisation qui accèdent au même réseau et aux mêmes ressources de données constitue un risque pour le Partenariat.

2.4.1 Sous réserve de l'autorisation de la direction et de l'équipe des TI, le Partenariat accepte que les employés apportent leurs propres appareils.

2.4.2 Tous les appareils mobiles doivent faire l'objet de mesures de gestion et de contrôles de sécurité des points terminaux.

2.4.3 Les appareils doivent être à jour et utiliser des systèmes d'exploitation récents; de plus, les derniers correctifs de sécurité doivent toujours être installés.

2.4.4 Les appareils peuvent faire l'objet d'une inspection et d'une surveillance active, et les droits d'accès seront révoqués s'il est déterminé que les appareils sont compromis.

2.4.5 Toutes les données du Partenariat sur des appareils mobiles doivent être chiffrées.

2.4.6 Il faut aviser immédiatement le bureau du fournisseur de services de gestion des TI ou l'équipe des TI du Partenariat si un appareil est perdu ou volé.

2.4.7 Tous les points terminaux doivent être gérés par des contrôles de sécurité des points terminaux approuvés.

2.5 Norme d'ouverture de session et de surveillance

La norme d'ouverture de session et de surveillance définit les exigences pour les événements d'ouverture de session de niveau « système » et les activités de surveillance de comptes dans le réseau organisationnel du Partenariat.

2.5.1 Les activités clés suivantes doivent être enregistrées :

i. la date de création de chaque ID utilisateur;
ii. la date et l'heure de la dernière ouverture de session, fermeture de session et ressource utilisée par un utilisateur;
iii. la date et l'heure du dernier changement de mot de passe pour chaque ID utilisateur;
iv. la date d'expiration (la dernière date à laquelle l'ID utilisateur a été utilisé);
v. les détails des privilèges ajoutés ou retirés de comptes utilisateur, le cas échéant;
vi. l'action effectuée par l'utilisateur et le moment où elle a été effectuée;
vii. tout accès à des dossiers ou à des données, ou modification de ceux-ci, dans la mesure du possible.

2.5.2 Les journaux doivent être configurés pour enregistrer les anomalies du système qui sont des indicateurs potentiels pour la détection d'attaques contre les systèmes du Partenariat ou de toute autre activité non autorisée.

2.5.3 Les journaux doivent être :

i. conservés pendant au moins un an et sauvegardés régulièrement, dans la mesure du possible, préférablement à un stockage sécurisé hors site;
ii. récupérés rapidement s'ils sont requis aux fins d'analyse;
iii. protégés contre des accès et des modifications non autorisés, préférablement en les conservant sur un serveur distinct hors de la zone démilitarisée (zone DMZ), comme un serveur de base de données protégé par un pare-feu, et être soumis à des restrictions d'accès au besoin; aucun

utilisateur ne devrait être en mesure de modifier ou de supprimer des renseignements du journal.

2.5.4 Les journaux doivent faire l'objet d'un suivi pour déterminer l'utilisation des ressources du système et détecter les événements de sécurité de l'information (tentatives infructueuses d'ouverture de session, ouvertures de session simultanées de différents endroits géographiques, élévation des privilèges, attaques contre les systèmes, etc.). Le logiciel de surveillance doit être configuré de manière à envoyer une alerte à l'équipe des TI s'il y a lieu.

2.5.5 L'exactitude des journaux dépend de l'exactitude de l'heure. Les systèmes qui contiennent ou traitent des renseignements confidentiels doivent être réglés de façon à synchroniser leurs horloges avec une source fiable. Ceux-ci doivent être synchronisés avec une source temporelle externe et une source temporelle de secours (plus d'une), comme ntp.org; tous les systèmes du Partenariat doivent utiliser ces sources ou un service équivalent comme source de synchronisation temporelle.

2.6 Norme de gestion des vulnérabilités

La **gestion des vulnérabilités** établit des contrôles et des processus pour détecter les vulnérabilités au sein de l'infrastructure de technologie et des composantes du système d'information de l'organisation qui pourraient être exploitées par des attaquants pour obtenir un accès non autorisé, perturber les activités opérationnelles et voler ou divulguer des données sensibles.

2.6.1 L'équipe des TI du Partenariat effectuera des analyses régulières des systèmes de production pour relever les vulnérabilités et communiquera toute vulnérabilité trouvée à l'équipe.

2.6.2 Pendant le cycle de vie d'élaboration du système, des analyses des vulnérabilités seront effectuées pour permettre la détection précoce de problèmes de sécurité.

2.6.3 Tous les systèmes d'usage externe seront analysés au moins tous les trimestres pour détecter les vulnérabilités.

2.6.4 La correction des vulnérabilités fera l'objet d'un suivi par l'équipe des TI, et elle sera surveillée et évaluée conformément à une norme de l'industrie, comme le Système commun de notation des vulnérabilités.

2.6.5 Sur demande, et dans le but d'effectuer une analyse ou une évaluation, l'autorisation d'accès nécessaire pour effectuer l'analyse ou l'évaluation sera accordée à des personnes désignées effectuant le travail. Cette autorisation ne comprendra pas l'accès direct à de l'information opérationnelle confidentielle ou à diffusion restreinte, ni à des renseignements personnels sans l'autorisation expresse écrite de l'agent en chef de la sécurité et de la protection des renseignements personnels du Partenariat.

2.6.6 Le Partenariat permettra l'accès aux locaux ou aux systèmes du Partenariat dans la mesure nécessaire pour effectuer la vérification ou l'évaluation autorisée. L'équipe des TI du Partenariat fournira les renseignements techniques nécessaires suffisants pour effectuer le travail. Voici les accès possibles :

i. accès niveau utilisateur ou accès niveau système aux systèmes du Partenariat;
ii. accès à l'information (information électronique, sur papier, etc.) qui peut être produite, transmise ou stockée sur les systèmes du Partenariat;
iii. accès aux aires de travail (bureaux, cubicules, zones de stockage, etc.);
iv. accès aux installations tierces qui hébergent les systèmes du Partenariat;
v. accès pour surveiller et enregistrer de manière interactive le trafic sur les réseaux du Partenariat.

2.6.7 Les activités de vérification ou d'évaluation pourraient influer sur la performance ou la disponibilité du réseau. Par conséquent, le Partenariat veillera à ce que toute activité qui pourrait nuire à la performance du système ou du réseau soit reportée après les heures de bureau.

i. Le Partenariat nommera une personne-ressource qui pourra donner suite aux enjeux, aux questions ou aux préoccupations concernant les problèmes ou les risques relevés pendant la vérification ou l'évaluation.
ii. Le Partenariat indiquera par écrit les dates et les heures de vérification ou d'évaluation.
iii. Les activités de vérification ou d'évaluation cesseront immédiatement si le Partenariat en fait la demande.

2.6.8 La correction des vulnérabilités suivra un flux de travail établi, tel que décrit dans l'**annexe C.**

2.7 Norme relative à la gestion des correctifs

La **gestion des correctifs** recense les contrôles et les processus visant à assurer la protection contre des menaces qui pourraient avoir une incidence négative sur la sécurité du système d'information ou des données confiées aux systèmes d'information. La mise en œuvre efficace de ces contrôles crée un environnement configuré de manière cohérente qui est protégé contre les vulnérabilités connues des systèmes de TI, du système d'exploitation et des logiciels d'application.

2.7.1 Tous les changements proposés aux systèmes d'exploitation, y compris les correctifs et les autres mises à jour, seront étudiés et, au besoin, testés avant la mise en œuvre pour garantir qu'il n'y ait pas d'effet négatif sur les applications prises en charge ou les contrôles de sécurité en place.

2.7.2 Les propriétaires de système seront responsables de surveiller la disponibilité et l'urgence connexe des correctifs communiqués par les fournisseurs pertinents. Dans tous les cas, lorsque des mises à jour sont appliquées aux systèmes d'exploitation, on étudiera la nécessité de mettre à jour le plan de continuité des activités et de reprise après sinistre.

2.7.3 Tous les systèmes seront régulièrement contrôlés pour détecter les mises à jour requises pour les systèmes d'exploitation et les versions des applications. Les correctifs seront installés sur tous les systèmes désuets selon un calendrier établi en fonction de la criticité de la mise à jour.

i. Les correctifs de sécurité seront traités avec beaucoup d'importance et appliqués aux systèmes dès que possible.

2.7.4 Tous les correctifs à installer seront soumis aux processus standards de gestion des changements pour garantir la planification de l'installation, le suivi et la mise en œuvre des correctifs sur tous les systèmes désignés.

2.7.5 Le processus de mise en œuvre de changements doit avoir une option de retour en arrière.

2.8 Norme de sauvegarde et de récupération des données

Des exigences de sauvegarde doivent être adoptées à l'échelle de tous les groupes opérationnels et de toutes les fonctions au sein du Partenariat. Cette norme définit des

méthodes acceptables pour la sauvegarde des données afin d'assurer la continuité des opérations du Partenariat en cas de perte des systèmes principaux de l'organisation.

2.8.1 Une évaluation des risques devra permettre de recenser les événements de sécurité de l'information et des TI susceptibles d'interrompre les processus opérationnels. Cette évaluation des risques peut être effectuée dans le cadre du processus d'évaluation des risques du Partenariat.

2.8.2 Le Partenariat doit veiller à ce que ses ressources informationnelles soient sauvegardées conformément aux besoins en matière de criticité opérationnelle, de continuité et de reprise après sinistre.

2.8.3 Le Partenariat tiendra un calendrier de sauvegarde documenté. Toutes les sauvegardes de données doivent être marquées et stockées dans des endroits sécurisés hors site.

2.8.4 Les systèmes opérationnels qui doivent faire l'objet d'une sauvegarde doivent être identifiés et documentés.

2.8.5 Tout lieu de stockage hors site doit seulement être accessible au personnel autorisé, en tout temps.

2.8.6 Seules les personnes autorisées peuvent retirer le support de sauvegarde et le transférer à l'emplacement de stockage.

2.8.7 Il faut définir les procédures à suivre pour récupérer les données du système opérationnel à partir du support de sauvegarde au système pertinent.

2.8.8 Des procédures d'essai de récupération des données de sauvegarde doivent être établies, et de tels essais doivent être effectués tous les deux ans pour confirmer l'efficacité du plan de récupération des données.

2.8.9 Pour connaître les périodes de conservation des supports de sauvegarde, il faut consulter la structure de classification de la gestion des documents et le calendrier de conservation du Partenariat.

2.8.10 Toutes les sauvegardes doivent être chiffrées.

2.8.11 Une méthode pour récupérer les supports de sauvegarde chiffrés, y compris pour gérer la clé de chiffrement, doit être définie.

L'exigence de conserver certains types de documents pendant une période donnée est pertinente pour protéger le Partenariat contre certaines pénalités ou amendes. En outre, ne pas se conformer à cette exigence pourrait entraîner la perte de droits, ou nuire aux litiges potentiels ou en cours en raison de la destruction de documents pertinents, et ainsi nuire à la position du Partenariat ou retarder les procédures. Pour plus d'information sur la politique et le calendrier

de conservation des documents du Partenariat, se reporter à la **structure de classification de la gestion des documents et au calendrier de conservation du Partenariat**.

2.9 Norme de reprise après sinistre

La norme de reprise après sinistre présente en détail les exigences de reprise, de secours et de non-interruption des services qui doivent être mises en œuvre par le fournisseur de services de gestion des TI du Partenariat et gérées par l'équipe des TI du Partenariat. Cette norme définit le processus pour la reprise après sinistre des activités du Partenariat en cas de perte des systèmes principaux de l'organisation.

2.9.1 Les plans de reprise après sinistre du Partenariat indiquent les personnes responsables de prendre des mesures raisonnables pour assurer la récupération des données sensibles et confidentielles.

2.9.2 Le Partenariat créera un plan de reprise après sinistre en vue d'élaborer des stratégies de récupération et de définir les données manquantes lors de la récupération.

2.9.3 Une fois ce plan créé, il sera mis à l'essai et mis à jour de manière régulière, au moins une fois par année, pour confirmer l'efficacité du plan.

2.9.4 Il doit être accessible aux personnes désignées, même lorsqu'elles travaillent de l'extérieur ou à distance.

2.9.5 Le plan de reprise après sinistre doit aborder les points suivants : environnement de la technologie de l'information, rôles et responsabilités, objectifs du point de récupération et objectif du temps de récupération.

2.10 Destruction des ressources et des données

La destruction physique et électronique sécurisée des données et des éléments informatiques ou des documents physiques est nécessaire à la protection des renseignements sensibles et personnels lorsque ceux-ci ne sont plus requis selon tout calendrier pertinent de rétention des documents.

2.10.1 L'information doit seulement être conservée pendant la durée requise, ou selon la durée prescrite par les lois ou règlements pertinents, le cas échéant.

2.10.2 Tous les employés du Partenariat sont responsables de veiller à ce que les données de l'organisation soient toujours supprimées d'un appareil avant le

transfert à une autre personne ou organisation, ou avant la mise au rebut. L'information doit être supprimée, même si elle ne semble pas être confidentielle ou sensible. Les employés doivent communiquer avec l'équipe des TI s'ils ont besoin d'aide pour la destruction des données.

2.10.3 Si un fournisseur de services tiers a reçu des copies de données organisationnelles, il doit détruire toute l'information en sa possession dans les sept jours suivant l'achèvement du projet ou la résiliation de l'accord, selon la première éventualité, en utilisant des méthodes de destruction conformes à la présente norme. Il doit ensuite remettre au directeur des technologies de l'information une confirmation de destruction signée dans un format conforme à cette norme.

2.10.4 Dans les cas où la destruction des données n'est pas possible, les gestionnaires et les directeurs peuvent consulter l'équipe des TI pour déterminer d'autres mesures de contrôle appropriées.

2.10.5 Toutes les méthodes suivantes sont acceptables pour la destruction des données :

i. utiliser un utilitaire logiciel comme « Secure Erase », qui efface, écrase ou chiffre les données;
ii. effacer magnétiquement (démagnétisation) les données;
iii. formater un appareil après avoir chiffré son contenu;
iv. utiliser une machine qui déforme ou détruit physiquement l'appareil pour empêcher la récupération des données.

2.10.6 Les fonctions « Vider la corbeille/poubelle », « Supprimer », « Retirer » ou « Formater » du système d'exploitation **ne détruisent pas** les données; ce ne sont donc **pas** des méthodes acceptables pour préparer un support en vue d'un transfert ou d'une mise au rebut.

2.10.7 Si on a recours au chiffrement avant le formatage d'un appareil, il faut respecter la norme de chiffrement avec des mots de passe ou des phrases passe robustes. Il est recommandé de compléter le chiffrement avec d'autres méthodes de destruction des données, dans la mesure du possible.

2.11 Norme relative aux pare-feu

Afin de garantir que le Partenariat ait une visibilité exhaustive du trafic sur son réseau, il faut s'assurer que tous les changements aux appareils réseau ou à leurs caractéristiques de sécurité sont pris en charge.

2.11.1 Tous les pare-feu installés doivent adopter le principe du « droit d'accès minimal » et refuser tout le trafic d'arrivée par défaut.
2.11.2 L'ensemble de règles doit être ouvert progressivement pour ne permettre que le trafic autorisé.
2.11.3 Les pare-feu doivent être installés dans les environnements où des « renseignements confidentiels » sont saisis, traités ou stockés.
2.11.4 Les ensembles de règles et les configurations des pare-feu doivent être revus et approuvés périodiquement chaque année pour garantir qu'ils offrent les niveaux de protection souhaités.
2.11.5 Ils doivent également faire l'objet de sauvegardes fréquentes sur différentes solutions de stockage. Plusieurs sauvegardes doivent être saisies et conservées afin de préserver l'intégrité des données, au cas où la récupération serait nécessaire. L'accès aux ensembles de règles, aux configurations et aux supports de sauvegarde doit être réservé à l'équipe des TI.
2.11.6 Les journaux administratifs des pare-feu du réseau (qui indiquent les activités administratives) et les journaux d'événement qui montrent le trafic doivent être tenus, conservés dans différentes solutions de stockage et examinés régulièrement. Un accès approprié aux journaux et aux copies est autorisé pour l'équipe des TI.
2.11.7 L'équipe des TI exécutera toute modification approuvée aux ensembles de règles des pare-feu par le biais du processus de gestion des changements.

2.12 Norme relative aux supports amovibles

Brancher un support de stockage amovible inconnu ou non géré entraîne plusieurs risques pour les systèmes et les données organisationnelles du Partenariat. Afin de garantir la protection des systèmes et des données du Partenariat, seuls les supports amovibles gérés ou approuvés aux fins d'utilisation par l'équipe des TI sont permis.

2.12.1 Les règles suivantes s'appliquent aux supports de stockage amovibles :
i. Les employés ne doivent pas copier des données confidentielles sur des supports de stockage amovibles.
ii. Les appareils dont le propriétaire n'est pas connu ne doivent pas être branchés aux systèmes du Partenariat.

iii. Tous les appareils fournis par des clients du Partenariat dans le cadre d'un engagement doivent être balayés pour rechercher les éléments malveillants.
iv. Le Partenariat doit mettre en œuvre des paramètres ou une politique de groupe pour interdire l'utilisation d'appareils amovibles non autorisés.
v. Tous les supports amovibles doivent être protégés par un mot de passe fort, ayant :
- au moins huit caractères;
- un mélange de chiffres et de lettres;
- au moins un caractère spécial;
- La biométrie peut être utilisée conjointement avec des mots de passe pour une authentification robuste;
- Les mots de passe écrits ne doivent pas être entreposés avec l'appareil.

2.12.2 Les appareils doivent être gérés centralement par le Partenariat.
2.12.3 Le Partenariat doit tenir un inventaire des appareils de stockage amovibles émis, y compris à qui l'appareil a été émis, et le statut de chiffrement de l'appareil.
2.12.4 L'information confidentielle ou à diffusion restreinte ne doit pas être stockée sur des supports de stockage amovibles à moins d'être chiffrée, conformément à la norme relative au chiffrement du Partenariat.
2.12.5 Les employés sont responsables de la sauvegarde et de la protection physique de tous les supports amovibles qui contiennent des renseignements confidentiels ou à diffusion restreinte.
2.12.6 Les appareils volés ou perdus contenant des renseignements confidentiels ou à diffusion restreinte doivent être signalés à l'équipe des TI, et ensuite à un partenaire dans les 24 heures. Les renseignements à fournir doivent comprendre :
i. Date du vol ou de la perte
ii. Description du vol ou de la perte
iii. Description de l'information stockée dans l'appareil
iv. Chiffrement ou non de l'appareil

2.13 Norme relative au chiffrement

La cryptographie est une méthode qui permet de stocker et de transmettre des données de façon à ce qu'elles puissent seulement être lues et traitées par les personnes auxquelles elles sont destinées. Le chiffrement est le processus qui permet de convertir des données de texte clair à un format qui n'est pas lisible par des parties non autorisées. Il prend également en compte ces données lorsqu'elles sont en mouvement, en cours de traitement et en stockage permanent.

2.13.1 Les données sensibles et confidentielles doivent être chiffrées conformément à la norme de classification des données.

2.13.2 Le Partenariat exige également le chiffrement lors de la transmission de données confidentielles par des canaux sécurisés.

2.13.3 Seuls les algorithmes de chiffrement approuvés par le gouvernement du Canada seront utilisés par le Partenariat[5].

2.13.4 À moins qu'ils n'aient été explicitement examinés par des experts indépendants qualifiés et approuvés par le directeur des technologies de l'information du Partenariat, on n'aura pas recours à des algorithmes de chiffrement propriétaires.

2.13.5 Le chiffrement est également exigé pour accéder à des données confidentielles par l'entremise de sites Web, d'applications Web, d'interfaces Web ou d'applications mobiles, d'une connexion VPN, FTP, d'un accès à distance, d'un bureau virtuel ou d'interrogations de base de données.

2.13.6 Des certificats SSL (*Secure Socket Layer*) délivrés par des autorités de certification tierces de confiance doivent être installés sur tous les serveurs Web du Partenariat. Les certificats autosignés doivent être restreints aux systèmes d'essai ou de développement.

2.13.7 Pour les systèmes qui doivent permettre l'accès ou l'administration à distance, un protocole SSH ou une technologie semblable doit être utilisé pour tous les accès administratifs.

2.14 Norme de sécurité du réseau

[5] Centre de la sécurité des télécommunications (« CSTC ») – Algorithmes cryptographiques pour l'information non classifié, protégé A et protégé B – https://cyber.gc.ca/sites/default/files/publications/itsp.40.111-fra.pdf

La norme de sécurité du réseau s'applique à tous les appareils réseau qui se connectent à l'infrastructure du réseau du Partenariat ou qui traitent de l'information confidentielle ou sensible, qu'ils fassent partie ou non de l'infrastructure du Partenariat.

Enregistrement des appareils

2.14.1 Avant de se connecter au réseau du Partenariat, tout appareil ou système doté d'une adresse IP doit être enregistré dans son inventaire de gestion des ressources et doit être conforme à la norme connexe.

Gestion de réseau

2.14.2 Des protocoles de texte en clair ne doivent pas être utilisés dans le cadre de la gestion de réseau.

2.14.3 Les protocoles de gestion de réseau simple (protocoles SNMP) par défaut doivent être modifiés.

2.14.4 Le trafic de gestion doit être séparé du trafic des utilisateurs.

2.14.5 L'accès aux interfaces de gestion des appareils réseau doit être à obtenu à l'aide d'un nom d'utilisateur et d'un mot de passe sécurisés, et par un réseau de gestion.

2.14.6 L'équipe des TI doit soumettre tout protocole initialement interdit à une procédure d'autorisation, et faire appel aux méthodes de chiffrement autorisées dans la norme relative au chiffrement.

Sauvegardes des appareils réseau

2.14.7 Seuls les employés autorisés doivent avoir accès aux sauvegardes de la configuration et aux commutateurs de configuration.

2.14.8 Tous les paramètres de configuration des appareils réseau doivent être sauvegardés régulièrement.

Exigences pour la transmission d'information confidentielle ou sensible

2.14.9 Toute transmission électronique de données confidentielles ou sensibles doit être conforme à la norme de classification des données et doit être chiffrée conformément à la norme relative au chiffrement et à la norme relative aux supports amovibles.

2.14.10 Le courrier électronique non chiffré n'est pas une méthode acceptable de transmission de renseignements confidentiels ou sensibles.

2.14.11 Tout message à destination ou en provenance d'un site qui n'est pas sous le contrôle du Partenariat ou de son réseau (p. ex. à destination et en provenance des fournisseurs ou des clients) doit être chiffré ou transmis par un tunnel chiffré avec des protocoles VPN ou SSL.

2.14.12 Il est interdit de transmettre de l'information par des applications Web, des protocoles ou des supports amovibles non approuvés (Dropbox, ShareFile, P2P, Google Drive, clés USB non gérées, etc.). L'acquisition de toute application Web doit être conforme à la norme relative aux services en nuage.

2.14.13 Des journaux de vérification doivent être tenus à jour pour toutes les transmissions d'information confidentielle ou sensible.

2.14.14 Dans la mesure du possible, il faut éviter de transmettre de l'information confidentielle ou sensible par documents papier.

i. Lorsqu'on ne peut pas éviter le papier, les copies d'information confidentielle ou sensible doivent être indiquées clairement selon leur classification de données (DIFFUSION RESTREINTE ou CONFIDENTIEL) et comme étant une COPIE.

ii. Les superviseurs doivent tenir à jour une liste de distribution des personnes auxquelles des copies ont été fournies.

2.15 Norme de protection des serveurs

La **norme de protection des serveurs** est maintenue par des mises à jour du système d'exploitation et des applications, par des mécanismes de contrôle des accès, et par des restrictions d'accès (utilisateurs, opérateurs et fournisseurs qualifiés et autorisés). L'intégrité, la confidentialité et la disponibilité des données doivent être maintenues.

2.15.1 Il faut tenir à jour une liste des applications fonctionnant sur chaque serveur, y compris le type et la version du système d'exploitation ainsi que les coordonnées des administrateurs, des propriétaires opérationnels et des gestionnaires de chaque serveur, et faire un suivi de cette information.

2.15.2 Les correctifs et les mises à jour d'application critiques doivent être appliqués.

2.15.3 La configuration du système d'exploitation doit être conforme aux lignes directrices approuvées en matière de sécurité des systèmes, lorsqu'elle est effectuée par le fournisseur du produit, ou conforme aux recommandations découlant d'une évaluation de la sécurité.

2.15.4 Un modèle ou une procédure de renforcement axé sur des rôles doit être établi, y compris :

i. Les services ou les programmes de gestion superflus du service doivent être retirés.
ii. Les logiciels superflus doivent être supprimés.
iii. Les paramètres de sécurité, la protection des fichiers et les journaux de vérification doivent être activés.
iv. Les comptes par défaut et les comptes d'invités doivent être désactivés, et les mots de passe doivent être changés, conformément aux exigences de la norme actuelle pour les mots de passe.
v. Les serveurs doivent être situés dans des environnements physiques sécurisés où on tient un registre des personnes ayant accédé à l'installation, et où le personnel non autorisé n'a pas accès.
vi. Les changements de serveur doivent être consignés dans un journal et effectués de manière conforme à la gestion des changements.

2.15.5 Tous les serveurs doivent disposer d'une protection des points terminaux et d'une protection contre les logiciels malveillants.

2.15.6 Tous les serveurs doivent être surveillés et leurs activités doivent être enregistrées.

2.15.7 Les serveurs doivent être séparés autant que possible, et l'accès doit seulement être permis aux personnes qui en ont besoin.

2.15.8 Les comptes de service et les autres comptes doivent avoir les droits d'accès minimaux requis pour effectuer les fonctions nécessaires précisées.

2.15.9 La capacité d'installer des logiciels et de modifier les journaux du serveur ne doit pas être détenue par un seul compte utilisateur.

2.16 Norme relative à la formation de sensibilisation à la sécurité

La formation de sensibilisation s'applique à tous les employés, sous-traitants et tiers du Partenariat. Ce sont souvent les personnes et non la technologie qui constituent la plus grande menace pour la sécurité et l'information. Le Partenariat fera tout son possible pour s'assurer que tous les employés, sous-traitants et tiers connaissent et respectent la norme.

La formation de sensibilisation est une activité permanente, et les utilisateurs doivent connaître les mesures qu'ils peuvent prendre pour assurer la protection de l'information, comme utiliser

un logiciel de sécurité, lutter contre les attaques d'ingénierie sociale, sauvegarder les données et signaler les infractions ou les incidents soupçonnés. La formation de sensibilisation *doit être interactive, comporter des simulations et permettre l'apprentissage à un rythme individuel*.

2.16.1 Tous les utilisateurs recevront une formation de sensibilisation à la sécurité dans une période donnée après avoir obtenu l'accès aux ressources du Partenariat. Cette formation peut être intégrée au processus d'intégration des nouveaux employés, et se poursuivre pendant toute la durée de leur emploi.

2.16.2 Les utilisateurs doivent être formés sur la façon de relever, de signaler et de prévenir les incidents de sécurité et les violations des données.

2.16.3 Ils doivent pouvoir consulter les politiques, les procédures et les manuels aux fins de référence.

2.16.4 Les utilisateurs doivent signer un document indiquant qu'ils reconnaissent avoir suivi la formation de sensibilisation à la sécurité.

2.16.5 L'équipe des TI doit tenir à jour la formation de sensibilisation à la sécurité et communiquer le nouveau contenu; elle doit notamment envoyer des rappels et tenir les utilisateurs au courant des menaces nouvelles et émergentes, et des pratiques exemplaires en matière de sécurité.

2.16.6 Les indicateurs de formation doivent être mesurés et déclarés.

3. FILTRES WEB

3.1 Norme relative aux filtres Web

Compte tenu du fait qu'il y a du contenu offensant, non professionnel ou inapproprié au lieu de travail disponible sur Internet, le Partenariat se réserve le droit de filtrer ce contenu par des contrôles d'accès ou la mise en œuvre d'une solution de filtrage Web pour interdire, séparer ou rejeter certaines pages Web pour les utilisateurs du réseau du Partenariat ou d'appareils fournis par le Partenariat.

3.1.1 L'équipe des TI surveillera l'utilisation Internet de tous les ordinateurs du réseau ainsi que de tous les appareils connectés au réseau organisationnel.

3.1.2 Les systèmes de surveillance du trafic doivent enregistrer l'adresse IP source, la date, l'heure, le protocole et le site ou le serveur de destination. Dans la mesure du possible, le système doit enregistrer l'ID utilisateur de l'utilisateur à l'origine du trafic.

3.1.3 Les journaux de filtres Web doivent être maintenus pendant une année.

3.1.4 Les membres de l'équipe mixte d'intervention en cas d'incident de sécurité informatique (EIISI) peuvent accéder à tous les rapports et à toutes les données s'ils en ont besoin pour répondre à un incident de sécurité de l'information.

3.1.5 Les gestionnaires et directeurs peuvent demander par écrit les rapports d'utilisation d'Internet de leur service au directeur de gestion des talents, aux fins de surveillance de la productivité des employés ou pour détecter toute infraction au présent Manuel de cybersécurité ou à la politique d'utilisation acceptable. Les rapports seront mis à la disposition de l'équipe des TI.

Si un site est filtré par inadvertance, les utilisateurs peuvent demander qu'il soit débloqué en soumettant un billet à l'équipe des TI. Un employé de l'équipe des TI examinera la demande et demandera au fournisseur de services de gestion des TI de débloquer le site, s'il est en effet mal classé.

Exceptions : Les employés peuvent accéder à des sites bloqués s'ils ont la permission de leur superviseur, et si cela est pertinent et nécessaire à des fins opérationnelles. Les superviseurs transmettront les demandes d'exception approuvées à l'équipe des TI par écrit ou par courrier électronique. L'équipe des TI débloquera ce site ou cette catégorie pour cet employé

seulement. L'équipe des TI fera un suivi des exceptions approuvées et en fera rapport sur demande. L'accès de l'employé sera désactivé lorsqu'il ne sera plus requis aux fins opérationnelles indiquées. Les exceptions suivies seront examinées tous les trimestres et approuvées par le superviseur de l'employé.

4. DÉTECTION DES INCIDENTS ET RÉPONSE

4.1 Norme de gestion des incidents de sécurité de l'information

La gestion des incidents détaille la prise en charge des incidents de sécurité des systèmes d'information. Cela comprend de communiquer aux utilisateurs les incidents de sécurité et les lacunes connexes qui doivent être traités. Cette norme permet une gestion efficace et efficiente des incidents en fournissant une définition et en établissant une structure de gestion et de production de rapports.

4.1.1 Tout incident dont on estimera qu'il pourrait porter atteinte à la sécurité de l'information devra être signalé, dans les meilleurs délais, à l'équipe des TI du Partenariat, qui transmettra le dossier au directeur des technologies de l'information ou à l'agent en chef de la sécurité et de la protection des renseignements personnels (ACSPRP), au besoin. Le cas échéant, ce dernier évaluera et qualifiera l'incident et produira un rapport destiné au PDG et au vice-président du secteur d'activité touché.

4.1.2 L'incident doit être évalué et pris en charge en conséquence par une réponse appropriée et proportionnée conformément à la procédure de réponse aux incidents de sécurité de l'information qui se trouve à l'*annexe D*.

4.1.3 Tous les renseignements sur l'incident, ses répercussions et la réponse doivent être consignés. Ils seront analysés, et l'impact de la réponse sera évalué. Les renseignements peuvent être consignés sur le formulaire fourni à l'*annexe E*.

4.1.4 Les membres de l'EIISI doivent être formés pour recueillir et conserver les renseignements sur tout incident, et pour produire des rapports.

4.1.5 On prescrira des mesures correctives en fonction du type et de la gravité de l'incident.

4.1.6 On pourra engager du personnel, des consultants et des sous-traitants en urgence afin qu'ils puissent contribuer aux efforts de rétablissement de la situation.

4.1.7 Dans tous les cas, la première réaction à la suite d'un incident ou d'une menace consistera à déterminer et à mettre en œuvre des mesures visant à les contenir ou à les minimiser. Il pourra notamment s'agir, à la seule discrétion du directeur des technologies de l'information ou de l'ACSPRP, de la mise hors

service de certaines parties des réseaux et des systèmes TI du Partenariat ou de la clôture de comptes utilisateur, et ce, avec effet immédiat.

Gestion des incidents liés à la protection de la vie privée

4.1.8 Lorsqu'il y a eu un incident de sécurité de l'information et qu'il est raisonnable de croire qu'il existe un risque réel de grave préjudice à l'endroit d'un individu en raison de la consultation, de la modification ou de la divulgation de renseignements personnels sous le contrôle du Partenariat, l'EIISI doit également suivre la **procédure de réponse aux incidents de violation de la vie privée** (qui se trouve à l'*annexe D*) pour garantir que les personnes touchées sont avisées et que l'incident est bien consigné et signalé.

5. CENTRE DE DONNÉES ET SÉCURITÉ PHYSIQUE

5.1 Norme relative à la sécurité physique des TI

Cette norme établit les règles pour contrôler, surveiller et retirer l'accès aux installations de centre de données de la TI du Partenariat, y compris les centres de données hébergés.

5.1.1 Une liste validée du personnel autorisé et le type d'accès requis doivent être revus régulièrement.
5.1.2 Tous les visiteurs doivent s'identifier, signer un registre, indiquer la nature de leur activité, nommer les personnes qu'ils sont venus voir et porter un insigne d'identification. Ils doivent signer le registre de nouveau au départ.
5.1.3 Les cartes ou les insignes d'accès ne doivent pas être partagés ou prêtés à d'autres.
5.1.4 Les cartes d'accès perdues ou volées doivent être signalées immédiatement à la sécurité des installations.
5.1.5 Les employés du Partenariat ainsi que ceux du fournisseur de services de gestion des TI du Partenariat doivent être vigilants et déclarer tout accès non autorisé soupçonné ou toute activité suspecte.

5.1.6 Les registres d'accès et les registres des visites doivent être conservés pendant au moins 12 mois et examinés périodiquement.

5.1.7 L'accès sera retiré lorsque les individus mettent fin à leur relation avec le Partenariat.

5.1.8 Les livraisons, l'accès de tiers, les réparateurs ou les autres visiteurs attendus en dehors des heures de travail normales doivent être autorisés à l'avance. Si aucun préavis n'est donné, ces personnes ne seront pas autorisées à entrer dans les installations du Partenariat.

5.1.9 Tous les serveurs du Partenariat doivent être situés dans des environnements physiques sécurisés où on tient un registre des personnes ayant accédé à l'installation, et où le personnel non autorisé n'a pas accès. Les serveurs ne doivent pas être exploités dans des espaces de bureaux publics; ils doivent se situer dans une installation de centre de données ou un laboratoire approuvé.

5.1.10 Les zones de travail du Partenariat devront être protégées par des contrôles d'entrée appropriés afin de garantir que seul le personnel autorisé peut y accéder. À titre d'exemple, les visiteurs et le personnel de service ne pourront pénétrer dans les zones de travail du Partenariat à moins d'être escortés par un membre du personnel.

6. FOURNISSEURS DE SERVICES EN NUAGE ET DE SERVICES TIERS

6.1 Norme relative à l'acquisition de services en nuage

Dans le cadre des activités opérationnelles du Partenariat, il est interdit de se procurer du matériel auprès de tiers non approuvés, ou d'en transmettre à ces tiers. Le Partenariat s'engage à tirer parti des applications en nuage pour offrir des services uniformes et sécurisés à l'organisation et aux services. Avant de conclure un marché avec un fournisseur de services en nuage, il faut :

6.1.1 Mener une évaluation générale des facteurs relatifs à la vie privée pour déterminer quels renseignements permettant d'identifier une personne, le cas échéant, sont stockés sur ce serveur, ou une évaluation générale des risques et des menaces pour relever les risques à la sécurité ou les vulnérabilités auxquelles le Partenariat pourrait être exposé.

6.1.2 Examiner les politiques et les procédures de sécurité actuelles utilisées par le service en nuage, y compris les certifications obtenues.

6.1.3 Déterminer ce qu'il advient des données stockées sur le serveur après la résiliation de l'entente.

6.1.4 Si le fournisseur de services en nuage ne permet pas au Partenariat de mener des évaluations indépendantes des vulnérabilités ou des tests de pénétration, il faut demander une copie de la vérification tierce la plus récente du fournisseur de services, comme un rapport SOC I ou II.

i. Après la passation de marché, le Partenariat doit demander ces types de rapport ou ces certifications tous les ans, s'ils sont disponibles :

- ISO 270XX
- FedRAMP
- Norme de sécurité des données de l'industrie des cartes de paiement
- Rapport de confiance et d'assurance de la Cloud Security Alliance
- Rapports de vérification SOC I ou II, ou certifications

6.1.5 S'assurer que toute entente entre le Partenariat et le fournisseur de services en nuage ou de services tiers contient des exigences de sécurité et de protection des renseignements personnels, ainsi que des rôles définis en matière de sécurité et de protection des renseignements personnels.

6.2 Norme relative aux services en nuage et aux services tiers

Afin de protéger la confidentialité, l'intégrité et la disponibilité du réseau opérationnel du Partenariat et des banques de données connexes, il faut s'assurer qu'aucun service en nuage ou autre service d'un tiers ne se connecte au réseau du Partenariat ou n'ait accès aux données du Partenariat sans l'autorisation de l'ACSPRP.

6.2.1 Il est interdit de contourner les processus d'authentification des utilisateurs sur tout appareil, système ou réseau du Partenariat afin de fournir l'accès à des fournisseurs de services en nuage ou à des fournisseurs tiers.

6.2.2 Les mots de passe et les éléments d'identification des utilisateurs ne doivent pas être communiqués aux fournisseurs de services en nuage ou de services tiers. Les données privées du Partenariat doivent demeurer sous le contrôle de l'organisation en tout temps. Les données opérationnelles ne doivent pas être communiquées à des tiers qui n'ont pas conclu d'entente contractuelle avec le Partenariat.

6.2.3 Il est interdit de connecter des appareils, des réseaux ou des systèmes qui n'appartiennent pas au Partenariat à ses réseaux sans l'autorisation de l'ACSPRP.

6.2.4 Les fournisseurs de services en nuage et de services tiers doivent convenir par écrit ou par contrat de veiller à ce que tout utilisateur, qu'il soit membre de leur personnel ou qu'il agisse à titre d'agent, s'engage à se conformer aux politiques applicables du Partenariat en matière de sécurité et de protection des renseignements personnels avant de recevoir une autorisation d'accès.

6.2.5 Toutes les connexions doivent utiliser des algorithmes et des protocoles de chiffrement, conformément à la norme relative au chiffrement.

6.2.6 Des procédures de gestion principales robustes sont requises.

6.2.7 Il est interdit d'exporter ou d'importer des logiciels, des données ou des solutions technologiques de fournisseurs de services en nuage ou de services tiers non autorisés.

6.2.8 Toutes les données stockées dans des services en nuage doivent être classées conformément à la norme de classification des données du Partenariat.

6.2.9 Dans la mesure du possible, le Partenariat doit stocker toutes les données dans des centres de données canadiens du fournisseur de services en nuage.

i. Si les fournisseurs de services en nuage n'ont pas de centres de données canadiens, des assurances contractuelles doivent être en vigueur pour garantir que le Partenariat garde le contrôle sur toutes les données stockées, et pour l'aviser immédiatement de tout accès non autorisé à ses données.

6.2.10 Des contrôles d'accès et des mesures de protection qui tiennent compte de la sensibilité des données stockées doivent être en place, et être conformes à la norme d'authentification des utilisateurs et des contrôles d'accès.

6.2.11 Les vulnérabilités et les correctifs doivent continuellement être gérés et surveillés, conformément aux normes de gestion des vulnérabilités et des correctifs. Ils peuvent être liés à la manière dont le service en nuage est utilisé, ou aux composantes de service sous la responsabilité du fournisseur.

i. Le fournisseur de services de gestion des TI du Partenariat est responsable d'appliquer tous les correctifs associés à l'infrastructure comme service (IaaS) du Partenariat.

6.2.12 Les services en nuage doivent être intégrés aux normes de sauvegarde et de reprise après sinistre du Partenariat.

6.3 Norme sur la sécurité des opérations liées aux services en nuage

En plus des mesures de protection en place aux centres de données des fournisseurs de services en nuage, il est essentiel qu'il y ait un niveau adéquat d'enregistrement et de déclaration, et que d'autres fonctions de sécurité soient disponibles et configurées pour la portée des services en nuage utilisés par le Partenariat.

6.3.1 Les services en nuage doivent permettre :

i. la détection rapide d'activités suspectes par les utilisateurs;
ii. la facilitation des enquêtes et des réponses aux incidents de sécurité;
iii. le soutien des fonctions de vérification;
iv. l'intégration et le respect des lignes directrices en matière de conservation des documents et de classification du Partenariat.

Gestion des incidents survenus chez un tiers

Le Partenariat doit pouvoir répondre à un incident de sécurité de l'information, même si cet incident s'est produit dans l'environnement du fournisseur de services en nuage, et ce, peu importe si le Partenariat a été directement touché ou non.

Le plan doit également tenir compte des utilisateurs tiers, des incidents de sécurité de l'information et des vulnérabilités connexes qui ont été signalés par des organismes tiers et le gouvernement, ainsi que des incidents de sécurité de l'information commerciaux et des organismes qui fournissent de l'information sur les vulnérabilités.

Si l'on attend des parties concernées qu'elles participent activement à la gestion des incidents de sécurité de l'information, il faut alors répartir clairement les rôles et les responsabilités et chacun doit en être conscient.

Sensibilisation et formation des tiers

La formation et l'éducation quant à la sensibilisation à la sécurité doivent être une priorité pour tous les tiers. Ils doivent être informés des politiques et des procédures de sécurité du Partenariat par rapport aux données et aux systèmes d'information.

Intégrité des données chez les tiers

La mise en œuvre d'une norme de sécurité tierce doit garantir l'intégrité des données, que celles-ci sont exhaustives et non modifiées, et que la source peut être vérifiée.

Confidentialité des données chez les tiers

Les tiers doivent garantir la confidentialité des renseignements sensibles et privés qui leur sont confiés par l'organisation.

Accords sur les niveaux de service (ANS) de tiers

Les deux parties doivent s'entendre sur les objectifs opérationnels de la relation et sur le résultat attendu de la part des services tiers. Les critères d'évaluation du risque des fournisseurs tiers doivent être définis. L'intégration des systèmes et des biens de TI doit faire partie de l'entente avec le tiers. Le processus pour les besoins en matière de transfert de données doit être abordé. Des évaluations continues doivent être établies, y compris des évaluations des risques, des tests de pénétration et des visites sur place.

Annexe A – MATRICE DES RESPONSABILITÉS EN MATIÈRE DE CYBERSÉCURITÉ DU PARTENARIAT

Le tableau suivant énumère plusieurs activités prescrites dans le Manuel de cybersécurité, la fréquence à laquelle elles doivent se produire, et la personne responsable de ces activités :

Politique ou norme	Activité	Fréquence	Responsabilité
Politique de cybersécurité	Révision du Manuel de cybersécurité et mise à jour de la politique de cybersécurité	Tous les deux ans	Directeur des technologies de l'information
Norme d'authentification des utilisateurs et des contrôles d'accès	Révision des droits d'accès des utilisateurs	Tous les trimestres	Gestionnaires et directeurs
	Révision des comptes partagés et des droits d'accès	Tous les trimestres	Directeur des technologies de l'information
	Modification des mots de passe dotés de privilèges de niveau « système » (super-utilisateurs, administrateurs, etc.)	Tous les ans	Équipe des TI
	Modification des mots de passe des utilisateurs	Tous les 90 jours	Tous les employés
Norme de sécurité des réseaux sans fil	Modification du mot de passe du réseau sans fil des invités	Tous les mois	Équipe des TI
Norme relative à l'accès à distance (réseau VPN) du Partenariat	Révision de l'accès à distance	Tous les trimestres	Gestionnaires de service et directeurs

Norme de sauvegarde et de récupération des données	Essai de la récupération des sauvegardes	Tous les trimestres	Équipe des TI
Norme relative à la reprise après sinistre et à la continuité des activités	Essai du plan de reprise après sinistre et du plan de continuité des activités	Tous les ans	Directeur des technologies de l'information
Norme de sécurité du réseau	Sauvegarde de la configuration des appareils réseau	Régulièrement	Équipe des TI
Norme relative aux filtres Web	Révision du besoin d'exceptions aux filtres Web	Tous les trimestres	Gestionnaires et directeurs

Annexe B – Processus d'évaluation des risques à la sécurité de l'information

Le processus d'évaluation des risques à la sécurité de l'information tient compte de ce qui suit :

Cote du niveau d'assurance par rapport au risque

L'information et les technologies de l'information du Partenariat peuvent être exposées à des risques précis. Les risques de TI peuvent être évalués en fonction de la **sensibilité** des banques de renseignements, de la **criticité opérationnelle** du service et de l'**exposition du point de vue de la sécurité** aux menaces.

Ce processus décrit la méthode du Partenariat pour déterminer le niveau d'assurance nécessaire à l'évaluation des risques de sécurité pour les nouvelles technologies et solutions. Il établit une **cote de risque** utilisée pour déterminer les **évaluations de la sécurité** nécessaires pour approuver un système aux fins de production.

La cote du niveau d'assurance sert à déterminer les exigences en matière de sécurité et d'approbation à respecter pour les nouveaux systèmes ou pour apporter des changements aux environnements technologiques actuels.

Cote du niveau de sensibilité

Le niveau de sensibilité sert à déterminer une valeur basée sur la sensibilité de l'information à une violation de la confidentialité ou de l'intégrité.

Niveau	Classification	Description	Exemples
1	Public	Renseignements accessibles au public, aux employés et aux entrepreneurs. « Données pour lesquelles il n'y a aucune attente relative à la vie privée ou à la confidentialité »	• Contenu du site Web • Rapports publiés • Matériels promotionnels • Offres d'emploi Présentations externes

Niveau	Classification	Description	Exemples
2	Interne/confidentiel	Renseignements accessibles au personnel et aux personnes autorisées ne faisant pas partie du personnel ayant un « besoin de savoir » pour des motifs professionnels Renseignements exclusivement accessibles aux personnes appartenant à un groupe particulier ou occupant une fonction ou un poste précis	• Documents de planification • Rapports d'avancement de projets • Ordre du jour et procès-verbal de réunions • Documents contenant des coordonnées professionnelles • Documents de planification stratégique • Documents opérationnels • Politiques et procédures • Conseils d'orientation stratégique • Fichiers du personnel • Renseignements bancaires de personnes ne faisant pas partie du personnel du Partenariat • Contrats • Rapports financiers • Délibérations et documents complémentaires du comité de direction du conseil d'administration • Autres comités du conseil d'administration • Renseignements des partenaires désignés comme étant de nature délicate • Renseignements commerciaux de tiers transmis avec la mention « Confidentiel »

Niveau	Classification	Description	Exemples
			• Renseignements sur les rémunérations • Conseils juridiques • Fichiers de signatures électroniques • Demandes de propositions et demandes de financement non attribuées • Enregistrements audio de réunions
3	À diffusion restreinte	Information sensible dont l'utilisation est réservée à des groupes précis d'employés. « Données régies par la loi; données qui permettraient l'accès à de l'information confidentielle ou à diffusion restreinte. Cela comprend les documents qui pourraient porter atteinte à la réputation ou mener à des ramifications juridiques s'ils faisaient l'objet d'une fuite (p. ex. renseignements permettant d'identifier une personne, données de carte de crédit, données des RH, et données stratégiques et financières). »	• Casiers et enquêtes judiciaires • Dossiers de procédure • Bases de données comme le registre du cancer, auxquelles seules les personnes désignées ont accès • Renseignements personnels sur la santé tels qu'ils sont décrits dans la *Loi sur la protection des renseignements personnels sur la santé de l'Ontario* (LPRPS)

Cote de criticité opérationnelle

La **disponibilité** d'une ressource se rapporte au degré de préjudice qui peut vraisemblablement résulter d'une destruction, d'une interruption ou d'un retrait non autorisé de toute **ressource** définie.

Niveau d'importance	Catégorie de système	Description
1	Opérationnel	Système qui pourrait être nécessaire au bon fonctionnement d'un certain secteur d'activité ou d'une certaine unité, ou qui nuirait à l'efficacité opérationnelle s'il n'était pas disponible, comme un système de temps et de présences ou les rapports de vente hebdomadaires.
2	Essentiel	Système qui, s'il n'était pas disponible, entraînerait des perturbations, des pertes financières ou des interruptions de fonctionnement au sein du Partenariat, comme la perte du courrier électronique ou du partage de fichiers.
3	Critique	Système qui, si sa disponibilité était compromise, pourrait causer un **préjudice élevé** au Partenariat, à ses partenaires ou à ses clients comme la perte de systèmes du point de vente, de la connectivité de réseau ou de systèmes de sécurité.

Cote d'exposition du point de vue de la sécurité

La valeur d'**exposition** a trait au degré d'exposition des systèmes aux menaces externes. Les menaces peuvent être accidentelles, malveillantes ou naturelles. Plus un système est exposé (p. ex. par une connexion Internet), plus il est probable qu'une ressource soit compromise.

Niveau d'exposition	Catégorie de système	Description
1	Systèmes internes	Systèmes internes à l'appui du Partenariat; aucun accès de l'extérieur de l'organisation et les systèmes sont isolés de manière logique – comme CCTV ou d'autres systèmes de surveillance de la sécurité.

Niveau d'exposition	Catégorie de système	Description
2	Extranet	Systèmes du Partenariat qui sont connectés au réseau interne, et qui sont seulement accessibles de l'extérieur de l'organisation par une connexion VPN sécurisée ou une protection équivalente.
3	Internet	Systèmes publics exposés à Internet.

Mesure des risques – Niveau d'assurance

Cette matrice des ressources indique le niveau d'assurance selon la cote globale de vulnérabilité.

Cote globale	Niveau d'assurance (NA)
3	-
4 ou 5	1
6 ou 7	2
8 ou 9	3

Produit livrable connexe	NA1	NA2	NA3
Suivi des risques dans le registre des risques de sécurité liés aux TI	✓	✓	✓
Intégration des ressources informationnelles dans l'évaluation des biens organisationnels (Énoncé de sensibilité)	✓	✓	✓
Microévaluation des risques et des menaces	✓	✓	✓
Exigences en matière de sécurité pour les documents		✓	✓

Produit livrable connexe	NA1	NA2	NA3
Acceptation des risques par les intervenants : Rapport sur les risques, plan de traitement		✓	✓
Vérification des mesures de protection et nouveau test Peut inclure l'exécution de tests de pénétration et d'évaluations des vulnérabilités.		✓	✓
Évaluation des répercussions sur les activités ou plan de reprise après sinistre Selon les exigences en matière de disponibilité		✓	✓
Matrice des exigences complètes en matière de traçabilité – Sécurité et protection des renseignements personnels		✓	✓
Évaluation indépendante des risques et des menaces Cette exigence peut être satisfaite par d'autres solutions, comme une vérification, une évaluation ou d'autres évaluations des risques et des menaces.			✓
Test de pénétration ou évaluation des vulnérabilités indépendants Cette information peut provenir d'autres tests, d'évaluations de vulnérabilité ou de tests mis à jour.			✓
Acceptation des risques par les dirigeants : Rapport sur les risques, plan de traitement			✓

Microévaluation des risques et des menaces

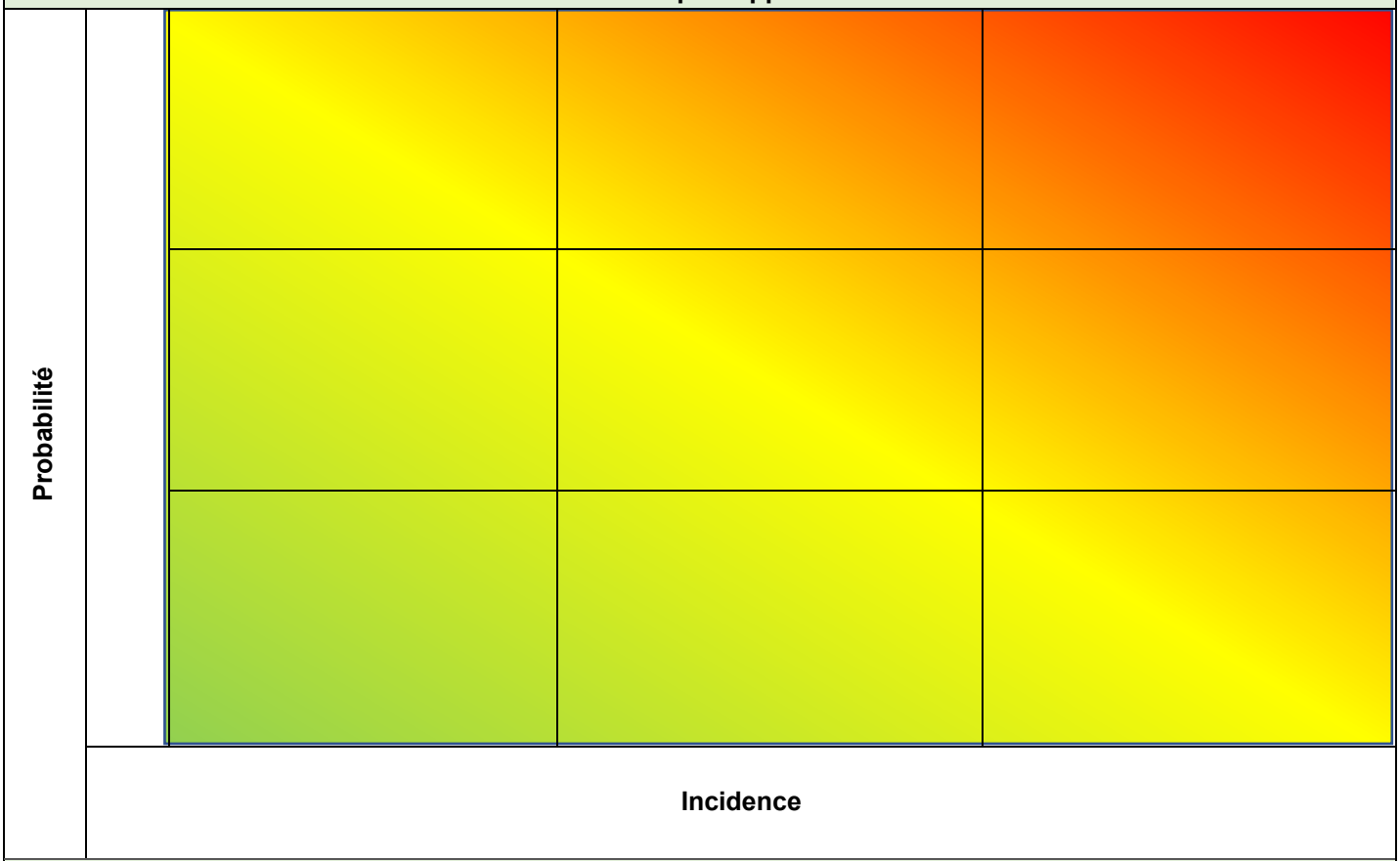
L'évaluation des risques vise à quantifier la mesure dans laquelle un risque donné est acceptable – c'est ce qu'on appelle la cote d'acceptation des risques. Les valeurs de vulnérabilité des ressources informent la valeur de risque résiduel, qui détermine globalement l'urgence liée à la mise en œuvre de mesures de protection pertinentes.

Titre de la solution		
Description de la solution		
Calcul du niveau d'assurance (3 à 9)		
Sensibilité	**Criticité**	**Exposition**
Public (1) ☐	Opérationnel (1) ☐	Systèmes internes (1) ☐
Interne/confidentiel (2) ☐	Essentiel (2) ☐	Extranet (2) ☐
Diffusion restreinte (3) ☐	Critique (3) ☐	Internet (3) ☐
RESSOURCE		
<Nom de la ressource>		
Description		
Confidentialité	**Intégrité**	**Disponibilité**
Le degré de préjudice qui peut vraisemblablement résulter d'une divulgation non autorisée.	Le degré de préjudice qui peut vraisemblablement résulter d'une destruction, d'une interruption ou d'un retrait non autorisé de toute **ressource** définie.	Le degré de préjudice qui peut vraisemblablement résulter d'une modification non autorisée, s'applique principalement à l'**information**.

Préjudice élevé

Vulnérabilités			
Vulnérabilité	**Catégorie**	**Description**	**Classement (1 à 3)**
	Ressource technique/ressource opérationnelle/ personnel/installations		

Tableau des ressources par rapport à la vulnérabilité



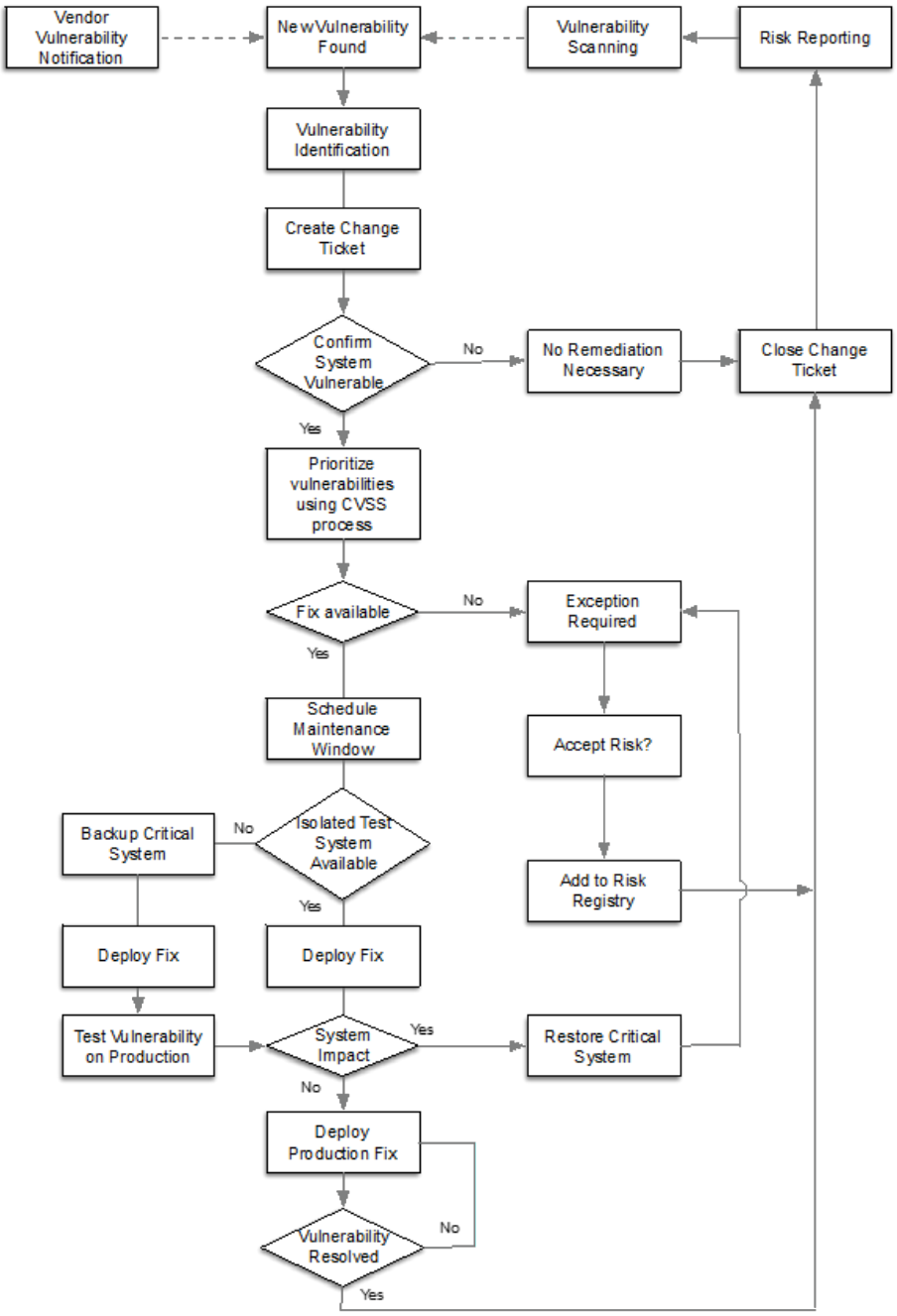
Risque		Recommandation(s)
Identificateur de risque		

Titre du risque		
Cote de risque		

Approbation

Le responsable du risque (cadre responsable) reconnaît la responsabilité de ce risque :	Acceptation des risques en matière de renseignements personnels et de sécurité :
Nom : _____ Signature	Nom : _____ Signature
Titre et nom de l'organisation Date	Titre et nom de l'organisation Date

Annexe C – Exemple de flux de travail pour la correction des vulnérabilités



Annexe D – Processus de réponse aux incidents de sécurité de l'information

La présente procédure de réponse aux incidents de sécurité de l'information établit une approche intégrée permettant aux fournisseurs de services de technologies de l'information (TI) du Partenariat et au Partenariat de réagir conjointement aux incidents de sécurité. Elle décrit les renseignements transmis au personnel concerné, l'évaluation de l'incident, la réponse intégrée, la documentation et la préservation des éléments probants.

Pour certains types d'incidents de sécurité de l'information, le Partenariat a élaboré des « guides » ou des processus à suivre par l'équipe des TI du Partenariat, le fournisseur de services de gestion des TI et l'EIISI.

Si l'équipe des TI du Partenariat détermine qu'un des événements précis suivants est survenu, le guide s'y rapportant doit être respecté, et non ce processus de réponse aux incidents :

- Incident lié à un logiciel malveillant (annexe XX)
- Incident lié à un logiciel rançonneur (annexe XX)
- Hameçonnage ou ingénierie sociale (annexe XX)

Détection et enregistrement de l'incident

Les incidents peuvent être découverts et signalés par un client, un membre du personnel, un partenaire ou un fournisseur du Partenariat. La personne qui découvre un incident doit immédiatement le signaler à l'équipe des TI, au directeur des technologies de l'information ou à l'ACSPRP.

Tous les employés du Partenariat recevant une alerte à propos d'un incident présumé ou confirmé, qu'ils fassent ou non partie de l'équipe des TI, devront s'efforcer de consigner, aussi clairement que possible, les renseignements suivants à propos de cet incident :

1. Le nom et les coordonnées de la personne qui a découvert l'incident
2. La date et l'heure de survenue de l'incident signalé
3. La nature de l'incident, le moment et les circonstances de sa détection
4. Les personnes physiques, les lieux et les systèmes informatiques concernés
5. Le nom du système ciblé, son système d'exploitation, son adresse IP et son emplacement
6. Tout renseignement sur l'origine de l'attaque, notamment, le cas échéant, des adresses IP
7. Une évaluation préliminaire de la gravité ou des répercussions de l'incident

Propriété, surveillance, suivi et communication des incidents

La propriété, la surveillance, le suivi et la communication des incidents relèveront, au premier chef, de la responsabilité du directeur des technologies de l'information, en collaboration avec le fournisseur de services de gestion des TI du Partenariat et les membres spécialisés de l'équipe mixte d'intervention en cas d'incident de sécurité informatique (EIISI).

Le directeur des technologies de l'information fera appel à des spécialistes des domaines concernés et formera une « équipe mixte d'intervention en cas d'incident de sécurité informatique » (EIISI) qui traitera des points suivants :

- L'incident est-il toujours en cours?
- Quelles données ou quels actifs sont menacés et quelle est la gravité de la menace?
- Quelles seraient les répercussions sur l'organisation si l'attaque réussissait?
- Quels sont les systèmes ciblés; quel est leur emplacement dans les locaux et sur le réseau du Partenariat?
- L'incident est-il survenu sur le réseau sécurisé?
- Une intervention urgente est-elle nécessaire?
- L'incident peut-il être contenu?
- De quel type d'incident s'agit-il (par exemple un virus, un ver, une intrusion, un usage abusif, un dommage, etc.)?
- Avec quel degré de confiance peut-on affirmer que l'on comprend pleinement la nature et les répercussions de l'incident?
- Est-il possible que des renseignements personnels sous le contrôle du Partenariat aient été consultés, modifiés ou divulgués? **Le cas échéant, consulter la procédure de réponse aux incidents liés aux renseignements personnels**.

On créera un rapport d'incident de sécurité. L'incident sera catégorisé selon le niveau le plus élevé applicable, conformément aux définitions ci-après.

Niveau I – Existence d'une menace pour la sécurité publique ou la vie.

Niveau II – Existence d'une menace pour les données

Niveau III – Existence d'une menace pour les systèmes informatiques

Niveau IV – Perturbation des services

Confinement

a. Les membres de l'EIISI suivront une procédure établie visant à contenir ou à minimiser les répercussions de l'incident, par exemple les procédures fournies au sein des logiciels antivirus.
b. S'il n'y a pas de procédure applicable, l'EIISI fera appel à des spécialistes du domaine, notamment externes, en vue de minimiser les répercussions de l'incident et documentera intégralement la procédure suivie.

c. Après la fin de l'incident, on communiquera cette procédure de manière appropriée afin de pouvoir y avoir recours lors de futurs incidents.

Résolution et rétablissement

a. Les membres de l'EIISI auront recours, afin de déterminer la cause de l'incident, à des techniques criminalistiques, notamment l'examen des journaux système, la recherche de lacunes dans la journalisation, l'examen des registres de détection d'intrusion et les interrogatoires de témoins.
b. Le personnel concerné, qui variera en fonction de l'incident, se verra accorder à ces fins un accès au système par le directeur des technologies de l'information.
c. Les membres de l'EIISI recommanderont la mise en œuvre de changements visant à empêcher la répétition d'un incident du même type et à prévenir sa propagation à d'autres systèmes. Ces changements seront mis en œuvre conformément à la Procédure de gestion du changement, ou pourront être réalisés en urgence. Les membres de l'équipe restaureront le ou les systèmes touchés dans leur état d'avant l'incident. Les tâches de restauration pourront inclure, sans que cela soit limitatif, les éléments suivants :
    i. Réinstallation complète du ou des systèmes touchés, accompagnée, s'il y a lieu, d'une restauration des données à partir des sauvegardes. Les membres de l'équipe pourront être tenus, avant de procéder à cette réinstallation, de conserver les éléments probants concernant l'incident.
    ii. Réinitialisation des mots de passe des utilisateurs ayant été compromis.
    iii. Vérification du renforcement du système grâce à la désactivation ou à la désinstallation des services non utilisés.
    iv. Vérification de la mise à jour du système sur le plan des correctifs.
    v. Vérification de l'activation de la protection en temps réel contre les virus et de la détection des intrusions.
    vi. Vérification de la journalisation des bons événements au niveau de détails approprié.

Documentation

Les renseignements suivants seront documentés au moyen du formulaire de rapport d'incident (*annexe E*). Il incombera au fournisseur de services TI du Partenariat de remplir ce rapport.

1. Tous les renseignements recueillis dans la section *Détection et enregistrement de l'incident* ci-dessus
2. La catégorie de l'incident (niveau I à IV)
3. Les circonstances de survenue de l'incident : par l'intermédiaire d'un courriel, d'un pare-feu, etc.
4. L'origine de l'attaque : par exemple une adresse IP ou le nom d'un ordinateur ou d'un utilisateur
5. D'autres renseignements relatifs à un attaquant potentiel
6. Le plan d'intervention, notamment les mesures préventives définies
7. Les mesures effectivement prises en réponse à l'incident
8. L'évaluation de l'efficacité globale de la réaction à l'incident

Conservation des éléments probants

S'il semble approprié de conserver les éléments probants, il pourrait être opportun, en conformité avec les sections ci-dessus, de recourir aux services d'un fournisseur tiers spécialisé dans les techniques criminalistiques et d'en informer le conseil juridique du Partenariat.
Dans le cas contraire :

- Conserver des copies des journaux, des courriels et des autres communications
- Établir une liste des témoins, de leurs déclarations et de leurs coordonnées
- Conserver tous les éléments probants jusqu'à ce que l'ACSPRP en décide autrement

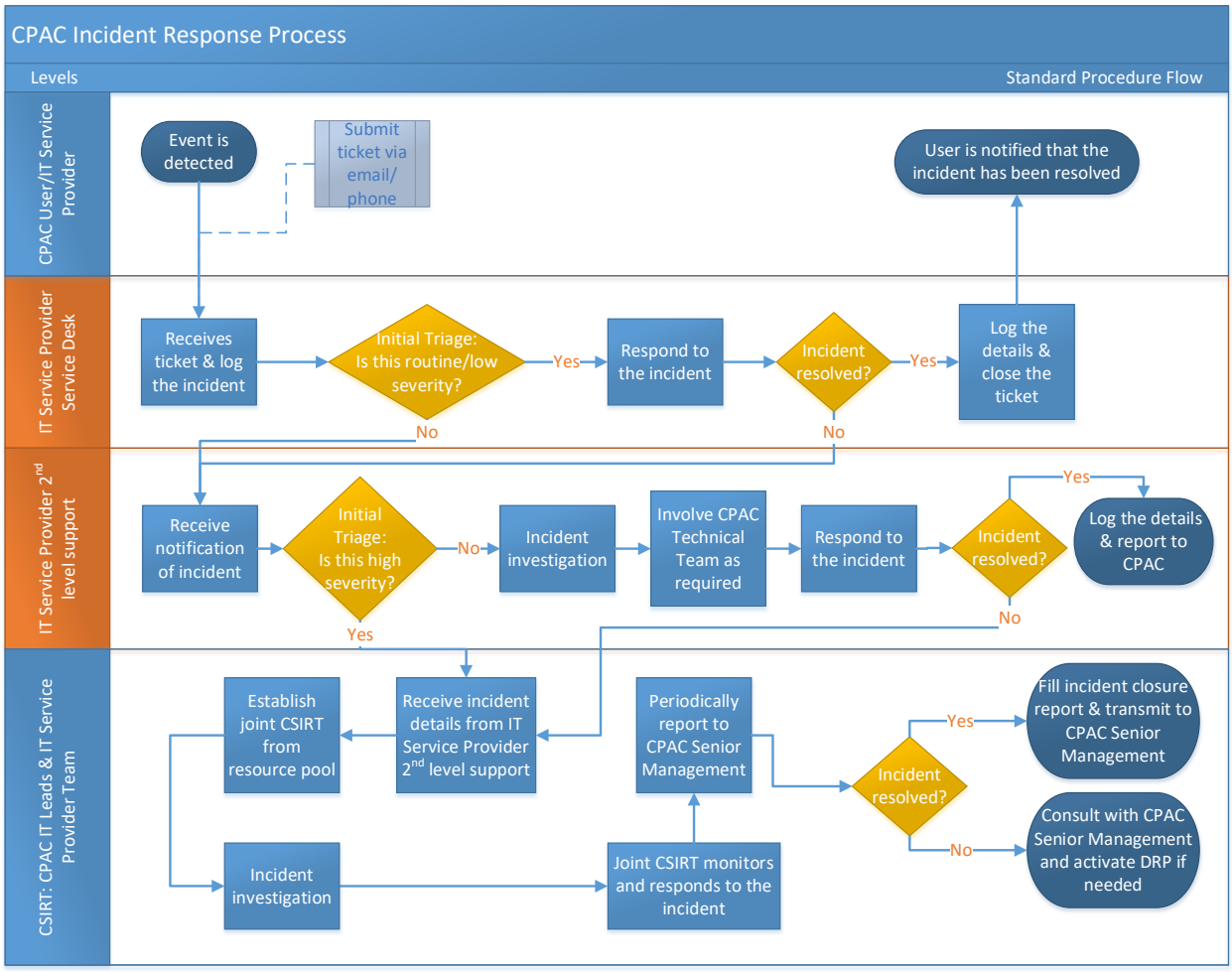
Rapport de clôture d'incident

Le fournisseur de services TI du Partenariat rédigera un rapport d'incident qui sera approuvé par le directeur des technologies de l'information et adressé en copie à l'ACSPRP. Outre les renseignements mentionnés ci-dessus, ce rapport contiendra :

i. Une évaluation des dommages et des coûts, un examen de la politique relative à la réponse aux incidents de sécurité de l'information et une version actualisée de toutes les politiques pertinentes, un plan de prévention de la répétition d'un incident similaire;
ii. Les exigences relatives aux politiques, procédures ou formations supplémentaires qui auraient pu empêcher ou atténuer les répercussions de l'incident;
iii. Une analyse de la pertinence et de la rapidité de la réponse et des possibilités d'amélioration en la matière;
iv. La disponibilité des spécialistes du domaine concerné pendant l'incident;
v. Toutes les autres leçons tirées de l'incident.

Procédure

Le processus de réponse aux incidents du Partenariat est décrit ci-dessous.



Annexe E– Formulaire de rapport d'incident de sécurité

RENSEIGNEMENTS D'IDENTIFICATION D'INCIDENT	
Numéro d'incident :	
Date et heure de la notification :	
Renseignements sur la personne ayant détecté l'incident :	
Nom :	Date et heure de détection :
Titre :	Lieu :
Téléphone et coordonnées :	Système ou application :

RÉSUMÉ DE L'INCIDENT

Type d'incident détecté :

☐Déni de service ☐Code ou logiciel malveillant ☐Utilisation non autorisée
☐Accès non autorisé ☐Violation ou vol de données ☐Autre

Description de l'incident :

Rôles des autres parties concernées :

NOTIFICATION D'INCIDENT – DIVERS

☐ Leadership TI ☐ Propriétaire du système ou de l'application ☐ Fournisseur du système ou de l'application
☐ Équipe d'intervention en cas d'incident de sécurité ☐ Équipe de direction ☐ Conseiller juridique
☐ Fournisseur de services externes ☐ Ressources humaines
☐ Autre :

MESURES

Mesures d'identification (vérification et évaluation de l'incident, évaluation des options) :

Mesures de confinement :
Recueil des éléments probants (journaux système, etc.) :
Mesures d'éradication :
Mesures de récupération (le cas échéant) :
Autres mesures d'atténuation :

ÉVALUATION
Évaluation de la pertinence de l'intervention de l'EIISI et des autres équipes
Les procédures documentées ont-elles été suivies? Étaient-elles adaptées?
Quels renseignements étaient requis en priorité?
Certaines mesures prises ont-elles pu empêcher le rétablissement?
Qu'est-ce que l'EIISI et le personnel informatique pourraient faire différemment la prochaine fois qu'un incident se produit?
Quelles mesures correctives pourraient prévenir la survenue d'incidents similaires dans le futur?

Quelles ressources supplémentaires seraient nécessaires pour détecter, analyser et atténuer de futurs incidents?

Autres conclusions ou recommandations :

SUIVI

Revu par :

☐ ACSPRP ☐ Service ou équipe informatique

☐ Directeur des technologies de l'information ☐ Autre

Mesures recommandées effectivement mises en œuvre :

Rapport initial rédigé par :

Suivi effectué par :

Annexe F – Guide opérationnel pour la gestion des ressources

La gestion des ressources signifie bien plus que simplement tenir à jour un inventaire des ressources appartenant au Partenariat. En cas d'incident de sécurité, un inventaire détaillé de la gestion des biens permettra au Partenariat de déterminer ce qui a été perdu, volé ou compromis, la sensibilité de l'information stockée dans les biens, et les appareils connectés au bien qui peuvent également avoir été touchés.

i. Il conviendra d'établir un inventaire de tous les actifs de l'organisation (matériels ou immatériels) associés à l'information et aux technologies de l'information et de le tenir à jour.
ii. Il conviendra de désigner des propriétaires de TI et des propriétaires opérationnels pour chacun des actifs associés au traitement et au stockage de l'information.
iii. Aucun nouveau bien essentiel en matière de systèmes d'information ne peut être acheté sans la participation du directeur des technologies de l'information.
iv. L'équipe des TI doit tenir un inventaire des technologies de l'information suivantes, détenues ou exploitées par le Partenariat :
    a. tous les systèmes d'information sur les lieux et à l'extérieur (ordinateurs portables et de bureau, serveurs, appareils mobiles, appareils réseau);
    b. tous les serveurs virtualisés.
v. L'inventaire des biens doit, au minimum, comprendre les détails suivants :
    a. nom du réseau auquel le bien est connecté;
    b. propriétaire du bien, ou responsable attitré;
    c. création du bien ou date de mise en œuvre;
    d. type de bien (station de travail, serveur, appareil mobile, machine virtuelle, interrupteurs, etc.);
    e. système d'exploitation du bien (Windows, Unix, etc.);
    f. version du système d'exploitation du bien (Windows 2016, RHEL X.x, Windows 10, etc.);
    g. état du bien (en utilisation, hors service, non utilisé);
    h. adresse IP (si elle est statique et disponible);
    i. numéro de série;
    j. sensibilité des données stockées sur l'appareil.