Procédure standard relative à la réponse aux incidents de sécurité de l'information

1.1 Aperçu

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) 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.

1.2 But

- Garantir une réaction rapide, documentée et contrôlée aux incidents de sécurité de l'information
- Vérifier qu'un incident s'est produit
- Maintenir ou restaurer la continuité des activités
- Minimiser les répercussions de l'incident
- Déterminer comment l'incident s'est produit et prévenir la survenue d'incidents similaires
- Améliorer la sécurité et la réaction aux incidents
- Tenir l'agent en chef de la sécurité et de la protection des renseignements personnels (ACSPRP) du Partenariat au courant de la situation et des interventions effectuées

1.3 Portée

Cette politique s'applique à l'ensemble du personnel, des consultants et des sous-traitants du Partenariat qui dirigent ou mettent en œuvre des interventions à la suite d'incidents de sécurité de l'information.

1.4 Énoncé de politique

I. Tout incident dont on estimera qu'il pourrait porter atteinte à la sécurité de l'information devra être signalé, dans les meilleurs délais, au directeur des technologies de l'information ou à l'ACSPRP. 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.

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

1.5 Rôles et responsabilités

On trouvera ci-dessous la description des rôles et des responsabilités des parties participant aux différentes étapes du processus de réponse à un incident. Pour de plus amples renseignements sur le protocole de communication, veuillez consulter la Procédure relative à la réponse et aux notifications en cas d'incident de violation de la vie privée.

1.5.1 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 découvrant un incident devra immédiatement communiquer avec le centre de services informatiques et avec l'ACSPRP.

Tous les employés du Partenariat recevant une alerte à propos d'un incident présumé ou confirmé, qu'ils fassent ou non partie du centre de services informatiques, 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

1.5.2 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 du Partenariat, en collaboration avec les fournisseurs de services TI et des spécialistes de la sécurité des systèmes concernés.

Le directeur des technologies de l'information du Partenariat 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?

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

1.5.3 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.

1.5.4 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.

1.5.5 Documentation

Les renseignements suivants seront documentés dans le formulaire de rapport d'incident ci-joint. 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'entremise 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

1.5.6 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

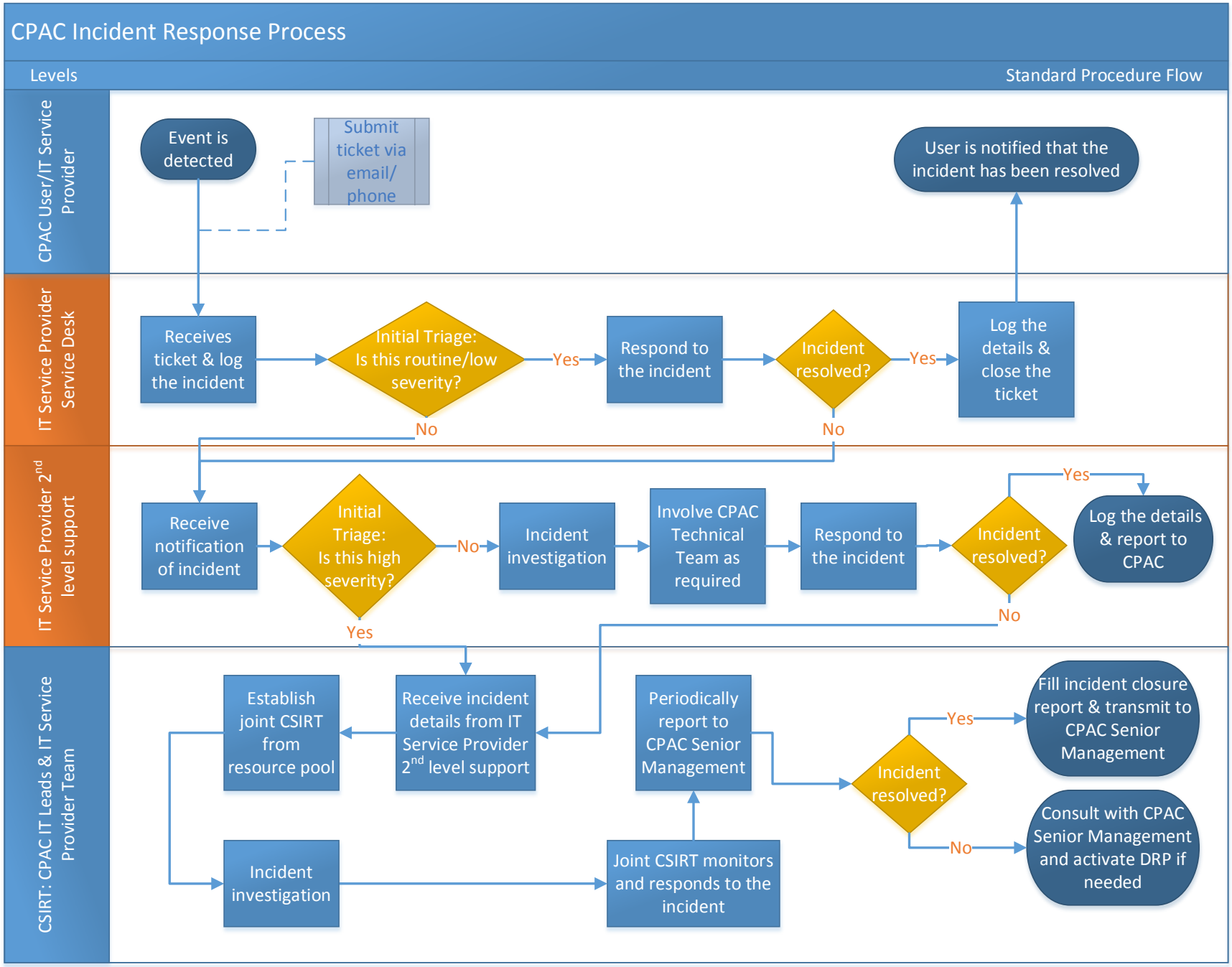
1.5.7 Rapport de clôture d'incident

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

1.6 Procédure

Les pages suivantes présentent le processus de réponse aux incidents du Partenariat.


CPAC Incident Response Process
Levels
Standard Procedure Flow
CPAC User/IT Service Provider
IT Service Provider Service Desk
IT Service Provider 2nd level support
CSIRT: CPAC IT Leads & IT Service Provider Team
Event is detected
Submit ticket via email/ phone
User is notified that the incident has been resolved
Receives ticket & log the incident
Initial Triage: Is this routine/low severity?
Yes
No
Respond to the incident
Incident resolved?
Yes
No
Log the details & close the ticket
Receive notification of incident
Initial Triage: Is this high severity?
No
Yes
Incident investigation
Involve CPAC Technical Team as required
Respond to the incident
Incident resolved?
Yes
No
Log the details & report to CPAC
Establish joint CSIRT from resource pool
Receive incident details from IT Service Provider 2nd level support
Incident investigation
Joint CSIRT monitors and responds to the incident
Periodically report to CPAC Senior Management
Incident resolved?
Yes
No
Fill incident closure report & transmit to CPAC Senior Management
Consult with CPAC Senior Management and activate DRP if needed

1.7 Contrôle de l'application de la politique

En cas de non-respect de cette politique, le Partenariat pourra, sans que cela soit limitatif, prendre les mesures suivantes :

i. Refuser l'accès à ses ressources informationnelles et TI.
ii. Mettre en œuvre, pour les fournisseurs indépendants, les consultants ou les sous-traitants, les recours contractuels appropriés, par exemple les dispositions relatives aux manquements au contrat ou à sa résiliation.
iii. Mettre en œuvre, pour le personnel, des mesures disciplinaires pouvant inclure, sans que cela soit limitatif, un avertissement écrit, une suspension avec ou sans traitement ou un licenciement immédiat motivé sans aucun préavis ni autre obligation.

1.8 Définitions

Terme	Définition
Ressources informationnelles et TI	Matériel informatique (y compris les ordinateurs portatifs et de bureau), logiciels, systèmes d'exploitation, supports de stockage, comptes réseau, courrier électronique, accès Internet, portails, passerelles, appareils réseau, appareils mobiles, serveurs, téléphones et systèmes téléphoniques, imprimantes multifonctions, ordinateurs et périphériques personnels et domestiques connectés au réseau du Partenariat, directement ou par l'entremise d'une connexion VPN, ressources informationnelles (quel que soit le support ou le format), par exemple les renseignements commerciaux ou personnels, ainsi que tout autre élément que le Partenariat pourrait considérer comme une ressource informationnelle ou TI
Incident de sécurité de l'information	Un incident de sécurité est une activité électronique ou physique pouvant entraîner ou menacer d'entraîner une perte de disponibilité, la compromission de l'intégrité ou la violation de la confidentialité des systèmes informatiques ou des renseignements du Partenariat. Des événements ou des actions peuvent être déclarés ou signalés comme constituant des incidents de sécurité avant toute violation effective ou toute répercussion. Des incidents de sécurité peuvent se produire à la suite d'une violation

Terme	Définition
	accidentelle ou délibérée des politiques de sécurité et des pratiques standard. Voici quelques exemples d'incidents de sécurité : • Pénétration ou attaque par déni de service de l'infrastructure réseau, des serveurs, des stations de travail, des applications et des sites Web • Accès non autorisé à des renseignements de nature délicate, personnels ou organisationnels, ou à des données des clients • Compromission de comptes utilisateur ou administrateur, ou de renseignements de connexion • Perte ou vol de dispositifs utilisés par les utilisateurs finaux, de périphériques de stockage amovibles, ou de copies papier de renseignements de nature délicate • Infection des systèmes informatiques du Partenariat par des logiciels malveillants • Attaques d'ingénierie sociale • Divulgation non autorisée de renseignements protégés par des moyens électroniques ou physiques • Utilisation des systèmes informatiques du Partenariat à des fins illégales telles que le lancement de cyberattaques, la distribution de matériel illicite ou le relais de pourriels • Autres violations des politiques du Cadre de sécurité et de protection des renseignements personnels du Partenariat
Adresse IP	Une adresse Internet Protocol (adresse IP) est une étiquette numérique attribuée à chaque périphérique (par exemple un ordinateur ou une imprimante) faisant partie d'un réseau informatique utilisant le protocole de communication Internet Protocol. Une adresse IP est plus communément représentée dans un format du type **172.16.254.1**, chacun des blocs de chiffres séparés par un point pouvant prendre n'importe quelle valeur entre 1 et 254.
EIISI	Équipe technique mixte établie entre le Partenariat et le fournisseur de services TI ayant pour mission d'intervenir à la suite d'un incident de sécurité et, s'il y a lieu, de

Terme	Définition
	solliciter des ressources externes en vue de résoudre ou de contenir l'incident et de rétablir la situation

1.9 Documents connexes

- Politique de classification des renseignements
- Politique d'utilisation acceptable
- Politique de protection des renseignements personnels
- Politique sur les appareils mobiles
- Politique de gestion de l'information
- Politique et procédures de gestion des dossiers
- Norme relative à la gestion des vérifications et de la vulnérabilité
- Norme relative à l'accès à distance et aux réseaux sans fil
- Norme relative au courrier électronique
- Norme relative à la sécurité de l'infrastructure TI
- Procédure relative à la réponse et aux notifications en cas d'incident de violation de la vie privée
- Politique de gestion des risques d'entreprise

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 :	Emplacement :
Téléphone et coordonnées :	Système ou application :

RÉSUMÉ DE L'INCIDENT

Type d'incident détecté :

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

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 rétablissement :
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 :

☐ Agent de sécurité
☐ Service ou équipe informatique
☐ Responsable de la protection des renseignements personnels
☐ Autre

Mesures recommandées effectivement mises en œuvre :

Rapport initial rédigé par :

Suivi effectué par :

Fin du document