CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

IR-08

Plan d'intervention en cas d'incident

Juill. 2026

Votre gouvernement

Québec

IR

Gestion des incidents de cybersécurité

Incident Response

IR-08 — Plan d'intervention en cas d'incident (PaFF)

Énoncés :

a. Élaborer un plan d'intervention en cas d'incident qui :

1. fournit à l'organisation une feuille de route pour la mise en oeuvre de ses capacités d'intervention en cas d'incident
2. décrit la structure et l'organisation des capacités d'intervention en cas d'incident
3. fournit une approche de haut niveau indiquant comment les capacités d'intervention en cas d'incident s'intègrent à l'organisation en général
4. répond à ses exigences spécifiques concernant sa mission, sa taille, sa structure et ses fonctions
5. définit les incidents devant être signalés
6. définit les paramètres de mesure de sa capacité d'intervention en cas d'incident
7. définit les ressources et le soutien de la direction nécessaires au maintien et à l'évolution de la capacité d'intervention en cas d'incident
8. décrit les modalités d'échange d'information en cas d'incident
9. est examiné et approuvé par [Affectation : personnel ou rôles définis par l'organisation] [Affectation : fréquence définie par l'organisation]
10. élabore explicitement la responsabilité de l'intervention en cas d'incident à l'intention de [Affectation : entités, personnel ou rôles définis par l'organisation]

b. Distribuer des copies du plan d'intervention en cas d'incident [Affectation : employées et employés (par nom ou rôle) et éléments organisationnels responsables de l'intervention en cas d'incident définis par l'organisation]
c. Mettre à jour le plan d'intervention en cas d'incident afin de tenir compte des changements apportés aux systèmes et des changements organisationnels, ou encore des problèmes rencontrés durant la mise en oeuvre, l'exécution ou la mise à l'essai du plan d'intervention
d. Communiquer les changements apportés au plan d'intervention en cas d'incident [Affectation : employées et employés (par nom ou rôle) et éléments organisationnels responsables de l'intervention en cas d'incident définis par l'organisation]
e. Protéger le plan d'intervention en cas d'incident des divulgations et des modifications non autorisées

Responsable : Aucun

Discussion :

Il est important que les organisations élaborent et mettent en oeuvre une approche d'intervention coordonnée en cas d'incident. La mission et les activités organisationnelles déterminent la structure des capacités d'intervention en cas d'incident. Dans le cadre des capacités d'intervention en cas d'incident, les organisations doivent considérer la coordination et l'échange d'information avec des organisations externes, y compris des fournisseurs de services et d'autres organisations participant à la chaîne d'approvisionnement. Pour ce qui est des incidents qui impliquent des renseignements personnels (par exemple, des atteintes à la vie privée) il convient d'inclure un processus permettant de déterminer si la transmission d'un avis aux organisations de surveillance ou aux personnes touchées est pertinente et de fournir cet avis en conséquence.