CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

PM-01

Plan du programme de sécurité de l'information

Juill. 2026

Votre gouvernement

Québec

PM

Gestion de programme à l'échelle organisationnelle

Program Management

PM-01 — Plan du programme de sécurité de l'information (PaFF)

Énoncés :

a. Élaborer et diffuser le plan d'un programme de sécurité de l'information panorganisationnel qui :

1. donne une vue d'ensemble des exigences liées au programme de sécurité et une description des contrôles de gestion du programme de sécurité et des contrôles communs qui ont été mis en place ou que l'on envisage de mettre en place en vue de satisfaire ces exigences

2. comprend l'identification et la répartition des rôles, les responsabilités, l'engagement de la direction, la coordination au sein des entités organisationnelles et la conformité

3. tient compte de la coordination parmi les entités responsables de la sécurité de l'information dans l'organisation

4. est approuvé par une ou un cadre supérieur ayant les responsabilités et la reddition de comptes nécessaires pour le risque qui pèse sur les activités organisationnelles (ce qui comprend la mission, les fonctions, l'image et la réputation), les biens organisationnels, les individus, les autres organisations et le gouvernement

b. Passer en revue et mettre à jour le plan du programme de sécurité de l'information panorganisationnel [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements définis par l'organisation]

c. Protéger le plan du programme de sécurité de l'information contre les divulgations ou les modifications non autorisées

Paramètres :

b.

1. triennale; lors de changements significatifs b.

2. annuelle; lors de changements significatifs

Responsable : OP

Discussion :

Le plan du programme de sécurité de l'information est un document officiel qui donne une vue d'ensemble des exigences de sécurité du programme de sécurité de l'information panorganisationnel et décrit les contrôles de gestion du programme et les contrôles communs qui ont été mis en oeuvre ou que l'on envisage de mettre en oeuvre pour satisfaire ces exigences. Le plan d'un programme de sécurité de l'information peut être représenté dans un seul document ou un ensemble de documents. Les plans du programme de protection de la vie privée et les plans de gestion des risques liés à la chaîne d'approvisionnement sont abordés séparément dans les contrôles PM-18 et SR-02 respectivement. Le plan d'un programme de sécurité de l'information documente les détails de la mise en oeuvre de la gestion du programme et des contrôles communs. Le plan fournit de l'information sur les contrôles (y compris la spécification explicite ou par référence des paramètres d'affectation et de sélection) pour permettre une mise en oeuvre clairement conforme à ses objectifs et la détermination des risques qu'il représente s'il est appliqué comme prévu. Les mises à jour apportées aux plans des programmes de sécurité de l'information comprennent des changements organisationnels et les problèmes relevés durant la mise en oeuvre du plan ou les évaluations de contrôles. Les contrôles de gestion des programmes peuvent être mis en oeuvre au niveau de l'organisation, de la mission ou du processus opérationnel, et sont essentiels à la gestion du programme de sécurité de l'information de l'organisation. Les contrôles de gestion des programmes se distinguent des contrôles hybrides, courants et propres aux systèmes, puisqu'ils sont indépendants de tout système particulier. Ensemble, les plans de sécurité de l'information individuels et le plan du programme de sécurité de l'information panorganisationnel fournissent une couverture complète des contrôles de sécurité employés dans l'organisation. Les contrôles communs dont les systèmes organisationnels peuvent hériter sont documentés dans une annexe du plan du programme de sécurité de l'information de l'organisation, à moins qu'ils ne soient compris dans le plan de sécurité distinct d'un système. Le plan du programme de sécurité de l'information panorganisationnel précise quels plans de sécurité distincts contiennent les descriptions des contrôles communs. Les événements qui peuvent précipiter une mise à jour du plan du programme de sécurité de l'information comprennent, sans s'y limiter, les conclusions d'une évaluation ou d'une vérification pangouvernementale, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices.