CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SI-01

Politique et procédures d'intégrité de l'information et des systèmes

Juill. 2026

Votre gouvernement

Québec

SI

Intégrité des systèmes et des données

System and Information Integrity

SI-01 — Politique et procédures d'intégrité de l'information et des systèmes (PaFF)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique d'intégrité de l'information et des systèmes [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

2. des procédures visant à faciliter la mise en oeuvre de la politique d'intégrité de l'information et des systèmes ainsi que des contrôles connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures d'intégrité de l'information et des systèmes

c. Passer en revue et mettre à jour, par rapport à l'intégrité de l'information et des systèmes :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Paramètres :

a. tout le personnel a.

1. organisationnel

b. chef de la sécurité de l'information organisationnelle c.

1. triennale; lors de changements significatifs c.

2. annuelle; lors de changements significatifs

Responsable : OP

Discussion :

La politique et les procédures d'intégrité de l'information et des systèmes abordent les contrôles de la famille SI qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures d'intégrité de l'information et des systèmes. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale de sécurité et de protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures d'intégrité de l'information et des systèmes comprennent les conclusions d'une évaluation ou d'une vérification, 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 applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.