CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SC-28

Protection de l'information au repos

Juill. 2026

Votre gouvernement

Québec

SC

Sécurité des communications et des systèmes

System and Communications Protection

SC-28 — Protection de l'information au repos (PaF-) (Obligatoire)

Énoncés :

Protéger [Sélection (un choix ou plus) : la confidentialité; l'intégrité] de l'information au repos suivante : [Affectation : information au repos définie par l'organisation].

Paramètres :

confidentialité et intégrité; minimalement : - les copies de sauvegarde - les journaux d'événements de sécurité

Responsable : OP

Date limite de mise en oeuvre : 2024-12-14

Discussion :

Par information au repos, on entend l'état de l'information lorsqu'elle n'est pas en cours de traitement, en transit ou stockée dans des composants du système. De tels composants comprennent les disques durs internes ou externes, les dispositifs réseau de stockage ou les bases de données. La protection de l'information au repos ne met toutefois pas l'accent sur le type de dispositif de stockage ou la fréquence d'accès, mais plutôt sur l'état de l'information. L'information au repos porte sur la confidentialité et l'intégrité de l'information, et concerne l'information relative aux utilisatrices et utilisateurs ainsi que celle relative aux systèmes. L'information relative aux systèmes nécessitant une protection comprend les configurations ou les ensembles de règles pour les pare-feu, les systèmes de détection et de prévention des intrusions, les routeurs de filtrage et le contenu d'authentification. Les organisations pourraient employer divers mécanismes pour assurer la protection de la confidentialité et de l'intégrité, y compris des mécanismes cryptographiques et l'analyse des échanges de fichiers. La protection de l'intégrité peut être assurée, par exemple, par la mise en oeuvre de technologies WORM (Write Once Read Many). S'il est impossible d'assurer une protection adéquate de l'information au repos d'une manière quelconque, les organisations peuvent utiliser d'autres contrôles, comme l'analyse fréquente pour relever le code malveillant au repos et le stockage hors site sécurisé plutôt que le stockage en ligne.