CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SC-13

Protection cryptographique

Juill. 2026

Votre gouvernement

Québec

SC

Sécurité des communications et des systèmes

System and Communications Protection

SC-13 — Protection cryptographique (PaF-) (Obligatoire)

Énoncés :

a. Déterminer les [Affectation : utilisations cryptographiques définies par l'organisation]
b. Mettre en place les types de cryptographies nécessaires à chaque utilisation cryptographique indiquée : [Affectation : types de cryptographies définis par l'organisation pour chaque utilisation cryptographique indiquée]

Paramètres :

a. utilisations cryptographiques, minimalement pour : applications ou sites Web exposés à Internet, appareils mobiles, journaux d'événements de sécurité (au repos), toutes données en transit et au repos
b. - recommandés (selon l'usage approprié) : HTTPS, version la plus récente de TLS, AES, SHA-2, cryptographie post-quantique - proscrits : tout protocole obsolète ou non sécuritaire (ex.: HTTP, SSL v2, SSL v3, TLS 1.0, TLS 1.1, etc.)

Responsable : OP

Date limite de mise en oeuvre : 2026-06-30

Discussion :

La cryptographie peut être employée pour soutenir une variété de solutions de sécurité, notamment la protection d'information classifiée et d'information protégée, la livraison et la mise en oeuvre de signatures numériques, et l'obligation de séparer l'information, lorsque des personnes autorisées disposent des habilitations requises pour l'information en question sans avoir les approbations formelles d'accès nécessaires. La cryptographie peut également servir à soutenir la génération aléatoire de nombres et la génération de hachage. Parmi les normes généralement appliquées en matière de cryptographie, on retrouve la cryptographie homologuée FIPS (Federal Information Processing Standard) et la cryptographie approuvée par le Centre pour la cybersécurité. Par exemple, les organisations qui doivent protéger l'information classifiée peuvent indiquer l'utilisation d'une cryptographie approuvée par le Centre pour la cybersécurité. Les organisations qui doivent fournir et mettre en oeuvre des signatures numériques peuvent indiquer l'utilisation d'une cryptographie homologuée FIPS. La cryptographie est mise en oeuvre conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables.