



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

CM-06

Paramètres de configuration

Juill. 2026



Gestion sécurisée des configurations système

Configuration Management

CM-06 – Paramètres de configuration (-F-)

Énoncés :

- a. Établir et documenter les paramètres de configuration des composants employés dans le système qui cadrent avec le mode le plus rigoureux sur le plan des exigences opérationnelles à l'aide de [\[Affectation : configurations sécurisées communes définies par l'organisation\]](#)
- b. Mettre en oeuvre les paramètres de configuration
- c. Déterminer, documenter et approuver tout écart en ce qui a trait aux paramètres de configuration établis pour [\[Affectation : composants de système définis par l'organisation\]](#) en tenant compte de [\[Affectation : exigences opérationnelles définies par l'organisation\]](#)
- d. Surveiller et contrôler les changements apportés aux paramètres de configuration conformément à ses stratégies et procédures

Paramètres :

- a. à définir par l'organisme
- c. à définir par l'organisme; à définir par l'organisme Informations additionnelles dans le contexte de l'administration publique du Québec : - les paramètres de durcissement exigés par le ministère de la Cybersécurité et du Numérique (MCN)

Responsable : Partagée

Discussion :

Les paramètres de configuration représentent les paramètres pouvant être modifiés dans les composants matériels, logiciels ou micrologiciels du système et qui affectent la posture de sécurité ou de protection de la vie privée ou encore le fonctionnement du système. Les produits de technologie de l'information pour lesquels il est possible de définir les paramètres de configuration comptent les ordinateurs centraux, les serveurs, les postes de travail, les systèmes d'exploitation, les appareils mobiles, les périphériques d'entrée et de sortie, les protocoles et les applications. Les paramètres qui ont une incidence sur la posture de sécurité des systèmes comprennent les paramètres de registre, les paramètres d'autorisation pour les comptes, les fichiers et les répertoires et les paramètres pour les fonctions, les ports, les services et les connexions distantes. Les paramètres de protection de la vie privée sont les paramètres qui ont une incidence sur la posture de protection de la vie privée des systèmes, y compris les paramètres nécessaires pour répondre à d'autres contrôles de protection de la vie privée. Les paramètres de protection de la vie privée incluent les exigences liées au contrôle d'accès, aux renseignements personnels, à la précision des données, aux capacités de manipulation des données, aux préférences de traitement des données et aux permissions de traitement et de rétention de l'information. Les organisations doivent établir des paramètres de configuration à l'échelle de l'organisation et par la suite des paramètres de configuration particuliers pour les systèmes. Les paramètres établis deviennent des éléments de la base de référence de la configuration pour le système. Les configurations sécurisées communes (que l'on appelle également les listes de vérification concernant la configuration de sécurité, les guides de confinement et de renforcement, et les guides de référence pour la sécurité) fournissent des points de repère reconnus, normalisés et établis qui stipulent les paramètres de configuration sécurisée associés à des plateformes ou à des produits de technologies de l'information ainsi que des instructions pour la configuration de ces produits afin de répondre aux exigences opérationnelles. Diverses organisations peuvent développer des configurations sécurisées communes, y compris les développeuses et développeurs de produits TI, les fabricants, les fournisseurs, les organismes gouvernementaux, les consortiums, le milieu universitaire, l'industrie ainsi que d'autres organisations des secteurs public et privé. La mise en oeuvre de configurations sécurisées communes peut être demandée au niveau organisationnel, au niveau du processus lié à la mission et aux activités; au niveau du système, ou à un niveau supérieur, y compris par un organisme de réglementation. Les configurations sécurisées communes comprennent les exigences de base en matière de sécurité pour les zones de sécurité de réseau (ITSP.80.022), les Common Criteria Evaluated Configuration Guides (en anglais), et les Security Technical Implementation Guides (STIG) du Department of Defense (DoD) des États-Unis, qui touchent la mise en oeuvre du contrôle CM-06 ainsi que d'autres contrôles comme AC-19 et CM-

07. Le protocole SCAP (pour Security Content Automation Protocol) et les normes qu'il définit offrent une méthode efficace et unique d'identification, de suivi et de contrôle des paramètres de configuration.