



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

AC-19

Contrôle d'accès pour les appareils mobiles

Juill. 2026



Gestion des droits d'accès aux systèmes et données

Access Control

AC-19 – Contrôle d'accès pour les appareils mobiles (PaF-) (Obligatoire)

Énoncés :

- a. Établir les exigences en matière de configuration et de connexion, ainsi que les directives de mise en oeuvre des appareils mobiles contrôlés par l'organisation à inclure lorsque ces appareils se trouvent à l'extérieur des zones contrôlées
- b. Autoriser les connexions d'appareils mobiles aux systèmes organisationnels

Paramètres :

aaQC. tablettes et téléphones doivent minimalement : - Respecter les exigences des mesures suivantes : AC-07, AC-19(05), AC-20(03), CM-06(01), CM-06(02) et SA-22; - Protéger les applications donnant accès aux données de l'organisme public par au minimum un NIP de six (6) caractères; - Cloisonner les applications donnant accès aux données de l'organisme public pour empêcher tout échange d'informations avec : - les autres applications de l'appareil mobile; - le stockage de l'appareil mobile autre que l'espace contenant les données de l'organisme public.

Responsable : OP

Date limite de mise en oeuvre : 2024-06-14

Discussion :

Un appareil mobile est un dispositif informatique de petite taille qui peut facilement être transporté par une personne. Il est conçu pour fonctionner sans connexion physique et il dispose d'un stockage de données local, fixe ou amovible. Il comprend également une source d'alimentation autonome. Les fonctionnalités des appareils mobiles peuvent également comprendre des capacités de communication vocale, des capteurs embarqués permettant aux appareils de recueillir des données et/ou des fonctions intégrées de synchronisation de données locales avec des emplacements distants. Les téléphones intelligents et les tablettes sont des exemples d'appareils mobiles. Les appareils mobiles sont typiquement associés à une seule personne et certains renseignements sont définis comme étant personnels. Par exemple, les appareils mobiles peuvent localiser l'accès en activant l'identification de la géolocalisation de l'utilisatrice ou utilisateur. De plus, comme certains appareils mobiles fournis à des fins professionnelles activent les profils personnels, les ministères gouvernementaux devraient mettre en place des stratégies et des procédures pour documenter la garde et le contrôle des transactions personnelles effectuées dans le profil personnel à partir de tels appareils. Les capacités de traitement, de stockage et de transmission de l'appareil mobile sont comparables à un sous-ensemble de postes de travail, selon la nature et l'utilisation prévue de l'appareil. La protection et le contrôle des appareils mobiles sont basés sur les comportements et les stratégies, et nécessitent que les utilisatrices et utilisateurs effectuent des opérations physiques afin de protéger et de contrôler leurs appareils lorsqu'ils se trouvent à l'extérieur des zones contrôlées. Les zones contrôlées sont des espaces dans lesquels les organisations appliquent des contrôles physiques ou procéduraux afin de respecter les exigences établies pour la protection de l'information et des systèmes. En raison de la grande variété d'appareils mobiles, y compris leur vaste gamme de caractéristiques et de capacités, les restrictions organisationnelles peuvent varier en fonction des classes ou des types d'appareils. Les restrictions d'utilisation et les conseils de mises en oeuvre propres aux appareils mobiles comprennent notamment la gestion des configurations, l'identification et l'authentification des appareils, la mise en oeuvre obligatoire de logiciels de protection, l'analyse des appareils afin de détecter les programmes malveillants, la mise à jour des logiciels antivirus, la recherche des mises à jour et des correctifs critiques, la vérification de l'intégrité du système d'exploitation de base et possiblement d'autres logiciels résidents, et la désactivation du matériel qui n'est pas nécessaire. Les restrictions concernant l'utilisation et l'autorisation d'accès peuvent varier selon les systèmes organisationnels. Par exemple, l'organisation peut autoriser la connexion des appareils mobiles à ses réseaux et imposer un ensemble de restrictions concernant l'utilisation, tandis qu'une ou un propriétaire de système peut refuser la connexion d'appareils mobiles à des applications en particulier ou imposer des restrictions additionnelles avant d'autoriser la connexion d'appareils mobiles à un système. Pour protéger adéquatement les appareils mobiles, il faut faire plus que se conformer aux exigences précisées dans le contrôle AC-

19. Plusieurs mesures de protection des appareils mobiles sont comprises dans d'autres contrôles. Le contrôle AC-20 porte sur les appareils mobiles qui ne sont pas contrôlés par les organisations. Le contrôle AC-08 dresse la liste des exigences relatives aux avis à envoyer par rapport à la collecte des renseignements personnels associés à l'utilisation de téléphones cellulaires professionnels fournis par le gouvernement.