



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

AC-16

Attributs de sécurité et de protection de la vie privée

Juill. 2026



Gestion des droits d'accès aux systèmes et données

Access Control

AC-16 – Attributs de sécurité et de protection de la vie privée (PaF-)

Énoncés :

- a. Fournir les moyens permettant d'associer les [Affectation : types d'attribut de sécurité et de protection de la vie privée définis par l'organisation] avec les [Affectation : valeurs des attributs de sécurité définies par l'organisation] pour l'information pendant qu'elle est stockée, traitée et/ou transmise
- b. S'assurer que toutes les associations d'attribut de sécurité sont effectuées et conservées avec l'information
- c. Établir les attributs de sécurité et de protection de la vie privée autorisés suivants à partir des attributs définis dans le contrôle AC-16A pour [Affectation : systèmes définis par l'organisation] : [Affectation : Attributs de sécurité et de protection de la vie privée définies par l'organisation]
- d. Déterminer les valeurs ou les plages autorisées des attributs suivants pour chacun des attributs définis : [Affectation : valeurs des attributs ou des plages définies par l'organisation pour les attributs définis]
- e. Vérifier les changements apportés aux attributs
- f. Examiner les [Affectation : attributs de sécurité et de protection de la vie privée définis par l'organisation] aux fins d'applicabilité [Affectation : fréquence définie par l'organisation]

Paramètres :

- a. profils de sécurité; sous-catégories
- c. tous les actifs informationnels; à définir par l'organisme en fonction de l'actif informationnel
- d. conformément aux sous-catégories des objectifs définis dans le modèle de classification de sécurité des données numériques gouvernementales
- f. profils de sécurité; lors d'un changement important au contexte de l'organisme Informations additionnelles dans le contexte de l'administration publique du Québec : - configurations et politiques de prévention de la perte de données sensibles standardisées par le ministère de la Cybersécurité et du Numérique (MCN)

Responsable : Partagée

Discussion :

L'information est représentée à l'interne dans les systèmes au moyen d'abstractions également appelées structures de données. Les structures de données internes peuvent représenter différents types d'entités actives et passives. Les entités actives, également appelées « sujets », sont habituellement associées à des personnes, à des dispositifs ou à des processus exécutés au nom des personnes. Les entités passives, également appelées « objets », sont habituellement associées à des structures de données comme des dossiers, des tampons, des fichiers, des canaux interprocessus et des ports de communications. Les attributs de sécurité (une forme de métadonnées) sont des abstractions des propriétés ou des caractéristiques d'entités actives et passives qui concernent la protection de l'information. Les attributs de protection de la vie privée, qui peuvent être utilisés de façon indépendante ou avec des attributs de sécurité, représentent les propriétés ou caractéristiques de base des entités actives ou passives en ce qui concerne la gestion des renseignements personnels. Les attributs peuvent être explicitement ou implicitement associés à l'information contenue dans le système de l'organisation ou ses composants. Ces attributs peuvent être associés à des entités actives (c'est-à-dire des sujets) qui ont le potentiel d'envoyer ou de recevoir de l'information, de faire circuler l'information entre des objets ou de changer l'état du système. Ils peuvent également être associés à des entités passives (c'est-à-dire des objets) qui contiennent ou reçoivent de l'information. L'association d'attributs à des sujets et objets s'appelle une liaison et fait habituellement partie de l'établissement de la valeur de l'attribut et de son type. Lorsqu'ils sont liés aux données ou à l'information, les attributs permettent de renforcer les stratégies de sécurité et de protection de la vie privée pour le contrôle de l'accès et du flux d'information, ce qui comprend les limites de conservation des données, les utilisations autorisées des renseignements personnels et l'identification des renseignements personnels dans les objets de données. Un tel renforcement s'effectue dans le cadre des processus organisationnels ou des fonctions ou mécanismes du système. Les techniques de liaison que les systèmes mettent en oeuvre nuisent à la force de la liaison entre les attributs et l'information. La force de la liaison et l'assurance associée aux techniques de liaison jouent des rôles importants dans la confiance qu'accordent les organisations au processus d'application du contrôle de flux d'information. Les techniques de liaison ont une incidence sur le nombre et le degré d'examen supplémentaires que devront exécuter les organisations. Le contenu ou les valeurs attribuées aux attributs peuvent avoir une incidence directe sur la capacité des personnes à accéder à l'information de l'organisation. Les organisations peuvent définir les types d'attributs requis pour que les systèmes appuient les fonctions liées à sa mission ou à ses activités. Plusieurs valeurs peuvent être assignées à un attribut de sécurité. En précisant les valeurs et les intervalles d'attribut permis, l'organisation s'assure que les valeurs d'attributs sont pertinentes et importantes. L'étiquetage désigne l'association d'attributs avec les sujets et objets représentés par des structures de données internes dans les systèmes. Il permet de faciliter l'application des stratégies de sécurité et de protection de la vie privée de l'information basées sur les systèmes. Les étiquettes comprennent la classification de l'information selon les exigences juridiques et de conformité (par exemple, TRÈS SECRET, SECRET, CONFIDENTIEL, PROTÉGÉ), le niveau d'incidence de l'information, l'information de bien de grande importance, les autorisations d'accès, la nationalité, la protection du cycle de vie des données (c'est-à-dire chiffrement et expiration des données), les autorisations de traitement des renseignements personnels, y compris le

consentement au traitement des renseignements personnels, et l'affiliation des entrepreneures et entrepreneurs. Le marquage est un terme associé à l'étiquetage. Il désigne l'association d'attributs à des objets dans une forme lisible par un humain et qui sont affichés sur les supports d'un système. Le marquage permet d'assurer une application manuelle ou basée sur les procédures ou les processus des stratégies de sécurité et de protection de la vie privée de l'information. Les étiquettes de sécurité et de protection de la vie privée peuvent avoir la même valeur que le marquage des supports (par exemple, TRÈS SECRET, SECRET, CONFIDENTIEL). Prière de consulter le contrôle MP-03 (Marquage des supports).