CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

AC-03(03)

Contrôle d'accès obligatoire

Juill. 2026

Votre gouvernement

Québec

AC

Gestion des droits d'accès aux systèmes et données

Access Control

AC-03(03) — Contrôle d'accès obligatoire (PbM-)

Énoncés :

Appliquer la [Affectation : stratégie de contrôle d'accès obligatoire définie par l'organisation] à l'ensemble de sujets et objets couverts qui sont définis dans la stratégie, quand la stratégie :
a. est appliquée de façon uniforme pour tous les sujets et objets dans le système
b. précise qu'un sujet ayant reçu l'accès à l'information est contraint :
- **1.** d'acheminer l'information à des sujets ou à des objets non autorisés
- **2.** d'octroyer ses droits d'accès à d'autres sujets
- **3.** de changer un ou plusieurs attributs de sécurité (précisés par la stratégie) pour des sujets, des objets, le système ou des composants du système
- **4.** de choisir les attributs de sécurité et les valeurs d'attribut (précisés par la stratégie) qui seront associés aux objets nouvellement créés ou modifiés
- **5.** de changer les règles régies par le contrôle d'accès

c. précise que les [Affectation : sujets définis par l'organisation] peuvent accorder explicitement [Affectation : droits d'accès définis par l'organisation], de façon à ce qu'ils ne soient pas limités par les contraintes ci-dessus

Responsable : Aucun

Discussion :

Le contrôle d'accès obligatoire est un type de contrôle non discrétionnaire des accès. Les stratégies de contrôle d'accès obligatoire limitent les opérations que peuvent exécuter les sujets par rapport à l'information obtenue des objets auxquels l'accès leur a déjà été accordé. C'est ce qui empêche les sujets de transmettre de l'information à des sujets ou à des objets non autorisés. Les stratégies de contrôle d'accès obligatoire limitent les opérations que peuvent exécuter les sujets en ce qui a trait à la propagation des privilèges de contrôle d'accès, à savoir qu'un sujet ayant un privilège ne peut pas le transmettre à d'autres sujets. La stratégie est appliquée de façon uniforme pour tous les sujets et objets que contrôle le système. Autrement, la politique de contrôle d'accès peut être contournée. Cette application est assurée par une mise en oeuvre qui répond au concept de contrôleur de référence décrit dans le contrôle AC-
25. La stratégie est délimitée par les frontières du système (c'est-à-dire une fois que l'information sort du contrôle du système, des moyens additionnels seront peut-être nécessaires pour s'assurer que les contraintes imposées sur l'information demeurent en vigueur). Les droits d'accès accordés aux sujets de confiance décrits ci-dessus sont conformes au concept du droit d'accès minimal (voir AC-06). Les sujets de confiance reçoivent seulement les droits d'accès minimaux qui sont nécessaires afin de satisfaire les besoins de l'organisation liés à la mission et aux opérations associées à la stratégie ci-dessus. Le contrôle s'applique particulièrement lorsqu'il existe un mandat qui établit une politique concernant l'accès à l'information protégée ou classifiée, où certaines utilisatrices ou certains utilisateurs du système ne sont pas autorisés à accéder à toute l'information sensible ou classifiée contenue dans le système d'information. Un contrôle d'accès obligatoire peut être appliqué en conjonction avec le contrôle d'accès discrétionnaire décrit dans le contrôle AC-03(04). Un sujet dont les activités sont limitées par les stratégies d'accès obligatoire peut quand même être en mesure de réaliser ses activités en vertu des contraintes moins rigoureuses du contrôle AC-03(04), mais les stratégies d'accès obligatoire ont préséance sur les contraintes moins rigoureuses du contrôle AC-03(04). Par exemple, bien qu'une stratégie de contrôle d'accès obligatoire impose une contrainte empêchant un sujet de transmettre de l'information à un sujet menant des activités à un niveau d'incidence ou de classification différent, le contrôle AC-03(04) permet au sujet de transmettre de l'information à des sujets ayant le même niveau d'incidence ou de classification que celui du sujet. Des exemples de stratégies de contrôle d'accès obligatoire comprennent la stratégie Bell-LaPadula pour protéger la confidentialité de l'information et la stratégie Biba pour protéger l'intégrité de l'information.