CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

AC-02

Gestion des comptes

Juill. 2026

Votre gouvernement

Québec

AC

Gestion des droits d'accès aux systèmes et données

Access Control

AC-02 — Gestion des comptes (PaF-) (Obligatoire)

Énoncés :

a. Définir et consigner les types de comptes permis et dont l'utilisation est interdite dans le système
b. Affecter des gestionnaires de comptes et des responsables des données
c. Exiger [Affectation : prérequis et critères ayant été définis par l'organisation] en ce qui concerne l'appartenance au groupe et au rôle
d. Préciser :
  1. les utilisatrices et utilisateurs autorisés du système;
  2. les membres des groupes et des rôles;
  3. les autorisations d'accès (par exemple, droits d'accès ou privilèges) et [Affectation : attributs définis par l'organisation (selon les besoins)] pour chaque compte
e. Obtenir l'approbation de [Affectation : personnel ou rôles définis par l'organisation] pour les demandes de création de comptes
f. Créer, activer, modifier, désactiver et retirer les comptes du système conformément aux [Affectation : politiques, procédures, conditions préalables et critères définis par l'organisation]
g. Surveiller l'utilisation des comptes
h. Aviser les gestionnaires de compte et [Affectation : personnel ou rôles définis par l'organisation] dans :
  1. [Affectation : délais définis par l'organisation] lorsque les comptes ne sont plus requis ou en état de latence
  2. [Affectation : délais définis par l'organisation] lorsque les utilisatrices et utilisateurs quittent leur emploi ou sont transférés
  3. [Affectation : délais définis par l'organisation] lorsque l'utilisation du système ou le besoin de connaître d'une personne change
i. Autoriser l'accès au système en fonction de ce qui suit :
  1. une autorisation d'accès valide
  2. l'utilisation prévue du système
  3. [Affectation : attributs définis par l'organisation (selon les besoins)]
j. Examiner périodiquement les comptes pour s'assurer qu'ils sont conformes aux exigences en matière de gestion des comptes tous les [Affectation : fréquence définie par l'organisation]
k. Établir et mettre en oeuvre un processus de changement des authentifiants de compte partagé ou de groupe (s'ils sont déployés) lorsque des utilisatrices et utilisateurs sont retirés du groupe
l. Aligner les processus de gestion des comptes avec les processus de cessation d'emploi et de mutation de personnel

Paramètres :

c. à définir par l'organisme d.
  3. à définir par l'organisme
e. détenteur de l'actif informationnel
f. à définir par l'organisme
h. détenteur de l'actif informationnel h.
  1. à définir par l'organisme en fonction du contexte h.
  2. à définir par l'organisme en fonction du contexte h.
  3. à définir par l'organisme en fonction du contexte i.
  3. à définir par l'organisme
j. au minimum 1 fois par année

Responsable : OP

Date limite de mise en oeuvre : 2021-06-30

Discussion :

Les types de comptes de système comprennent les comptes individuels, partagés, temporaires, anonymes ou d'invité, de groupe, de système, d'urgence, de développeuse ou développeur et de service. L'identification des utilisatrices et utilisateurs autorisés du système et la spécification des privilèges d'accès reflètent les exigences que l'on retrouve dans d'autres contrôles de sécurité et de protection de la vie privée. Les utilisatrices et utilisateurs nécessitant des privilèges administratifs sur les comptes du système font l'objet d'un examen plus approfondi de la part des responsables du personnel de l'organisation pour l'approbation des comptes et de l'accès privilégié. Il peut s'agir entre autres de la ou du propriétaire du système, de la mission ou des activités, d'une ou un cadre supérieur de la gouvernance en matière de sécurité du ministère, d'une ou un responsable des données ou d'une haute ou un haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée. Les types de comptes que les organisations peuvent interdire en raison d'un risque de sécurité accru incluent les comptes partagés, anonymes, temporaires, de groupe, d'urgence et d'invité. Dans la mesure où l'accès comporte des renseignements personnels, les cadres supérieures et supérieurs responsables de la sécurité et de la protection de la vie privée collaborent avec la ou le responsable des données pour déterminer les conditions particulières de l'appartenance aux groupes et aux rôles, identifier les utilisatrices et utilisateurs autorisés,

l'appartenance aux groupes et aux rôles, et les autorisations d'accès pour chaque compte, ainsi que créer, ajuster ou supprimer les comptes du système conformément aux stratégies organisationnelles. Les stratégies peuvent comprendre de l'information telle que les dates d'expiration des comptes ou d'autres facteurs qui déclenchent la désactivation des comptes. Les organisations peuvent choisir de définir les droits d'accès ou d'autres attributs en fonction du compte, du type de compte ou d'une combinaison des deux. Les exemples d'autres attributs requis pour autoriser l'accès incluent les restrictions en fonction du moment de la journée, du jour de la semaine et du point d'origine. Au moment de définir les autres attributs des comptes de système, les organisations considèrent les exigences liées au système et celles liées à la mission ou aux activités. Si les organisations ne considèrent pas ces facteurs, la disponibilité des systèmes risque d'en subir les conséquences. Les comptes temporaires et d'urgence devraient être utilisés à court terme. Les organisations établissent des comptes temporaires dans leurs procédures standard d'activation de compte s'il convient d'utiliser les comptes à court terme et que leur activation n'est pas urgente. Les organisations établissent des comptes d'urgence à la suite de situations de crise et lorsqu'il faut activer des comptes rapidement. Par conséquent, l'activation de compte d'urgence risque de contourner les processus standard d'autorisation de compte. Il ne faut pas confondre les comptes temporaires et d'urgence avec les comptes utilisés peu fréquemment, notamment les comptes d'ouverture de session locaux utilisés pour réaliser des tâches particulières ou lorsque les ressources réseau ne sont pas disponibles (communément appelés des comptes de dernier recours). Ces comptes demeurent activés et ne sont pas assujettis aux dates de retrait ou de désactivation automatique. Les conditions de désactivation des comptes peuvent inclure ce qui suit : lorsque les comptes temporaires, les comptes d'urgence ou les comptes partagés ou de groupe ne sont plus requis; ou lorsque des utilisatrices ou utilisateurs quittent leur poste ou font l'objet d'un transfert. Changer des authentifiants partagés ou de groupe vise à s'assurer que d'anciennes ou anciens membres du groupe ne puissent pas conserver des accès au compte partagé ou de groupe. Les utilisatrices et utilisateurs de certains types de comptes de système pourraient être appelés à suivre une formation spécialisée.