CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

IA-05

Gestion des authentifiants

Juill. 2026

Votre gouvernement

Québec

IA

Contrôle de l’identité et de l’authentification

Identification and Authentication

IA-05 — Gestion des authentifiants (PaF-) (Obligatoire)

Énoncés :

Gérer les authentifiants de système des façons suivantes :
a. vérifier, au moment de la distribution initiale d'un authentifiant, l'identité de l'utilisatrice ou utilisateur, du groupe, du rôle, du service ou du dispositif recevant l'authentifiant
b. établir le contenu de l'authentifiant initial pour les authentifiants émis par l'organisation
c. s'assurer que le mécanisme d'authentification est suffisamment robuste pour l'utilisation prévue
d. établir et mettre en oeuvre des procédures administratives pour la distribution initiale des authentifiants en cas de perte, de compromission, de corruption et de révocation
e. changer les authentifiants par défaut lors de la première utilisation
f. modifier ou actualiser les authentifiants [Affectation : durée définie par l'organisation selon le type d'authentifiant] ou quand [Affectation : événements définis par l'organisation] se produisent
g. protéger le contenu des authentifiants contre les divulgations ou les modifications non autorisées
h. exiger que les personnes et les dispositifs appliquent des contrôles particuliers de manière à protéger les authentifiants
i. modifier les authentifiants pour les comptes de groupes ou de rôles lorsque des changements sont apportés à leurs membres

Paramètres :

f. - mots de passe : au moins à tous les 180 jours - certificats : à chaque année; un événement de sécurité survient ou au besoin

Responsable : OP

Date limite de mise en oeuvre : 2025-04-30

Discussion :

Les authentifiants comprennent les mots de passe, les dispositifs de chiffrement, la biométrie, les certificats, les dispositifs avec mot de passe à usage unique et les cartes d'identité. Les authentifiants de dispositif comprennent les certificats et les mots de passe. Le contenu de l'authentifiant initial correspond au contenu réel de l'authentifiant (par exemple, le mot de passe initial). Comparativement, les exigences pour le contenu de l'authentifiant contiennent des caractéristiques ou critères particuliers (par exemple, longueur minimale des mots de passe). Les développeuses et développeurs peuvent livrer des composants de systèmes avec les justificatifs d'authentification (c'est-à-dire les mots de passe) pour l'installation et la configuration initiales. Les justificatifs d'authentification par défaut sont souvent bien connus, faciles à découvrir et présentent un risque important. Les exigences de protection des authentifiants de personnes peuvent être appliquées par les contrôles PL-04 ou PS-06 pour les authentifiants qui se trouvent dans la possession de personnes et par les contrôles AC-03, AC-06 et SC-28 pour ceux qui sont stockés dans les systèmes organisationnels, comme des mots de passe stockés sous forme hachée ou chiffrée, ou des fichiers contenant des mots de passe hachés ou chiffrés accessibles à l'aide de privilèges d'administrateurs. Les systèmes prennent en charge la gestion des authentifiants de personnes en fonction des paramètres et des restrictions définis par l'organisation pour différentes caractéristiques d'authentifiants (par exemple, la longueur minimale des mots de passe, la fenêtre de validation des jetons à utilisation unique et le nombre de rejets permis durant le stade de vérification d'une authentification biométrique). Il est possible de mettre en oeuvre des mesures pour protéger les authentifiants individuels, y compris garder les authentifiants en sa possession, ne pas les partager avec d'autres personnes et signaler immédiatement leur perte, leur vol ou leur compromission. La gestion des authentifiants comprend l'émission et la révocation des authentifiants pour un accès temporaire, qui ne sera plus nécessaire par la suite.