CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SA-08(27)

Sécurité tenant compte du facteur humain

Juill. 2026

Votre gouvernement

Québec

SA

Acquisition sécurisée des systèmes/services

System and Services

SA-08(27) — Sécurité tenant compte du facteur humain (PbMM)

Énoncés :

Mettre en place le principe de conception sécurisée de la sécurité tenant compte du facteur humain dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de la sécurité tenant compte du facteur humain repose sur le fait que l'interface utilisateur des fonctions de sécurité et des services de soutien est intuitive et conviviale et qu'elle permet de fournir une rétroaction des actions effectuées par les utilisatrices et utilisateurs qui ont une incidence sur une telle stratégie et son application. Les mécanismes qui permettent d'appliquer la stratégie de sécurité ne sont pas intrusifs pour les utilisatrices et utilisateurs et sont conçus de manière à ne pas nuire à l'efficacité de ces derniers. Les mécanismes d'application des stratégies de sécurité offrent également aux utilisatrices et utilisateurs une rétroaction claire, utile et pertinente et des avertissements lorsque des choix non sécurisés sont effectués. Une attention particulière est accordée aux interfaces par l'entremise desquelles le personnel responsable de l'administration et de l'exploitation des systèmes configure et met en place les stratégies de sécurité. Idéalement, les membres du personnel devraient être en mesure de comprendre les conséquences de leurs choix. Le personnel qui assume des responsabilités d'administration et d'exploitation de systèmes est en mesure de configurer les systèmes avant leur démarrage et de les administrer lors de leur exécution tout en étant persuadé que ses intentions ont bien été prises en compte dans les mécanismes des systèmes. Les services, les fonctions et les mécanismes de sécurité ne nuisent pas à l'utilisation prévue du système et ne compliquent pas son utilisation inutilement. Il convient de faire un compromis entre l'utilisabilité du système et la robustesse nécessaire pour appliquer les stratégies de sécurité. Si les mécanismes de sécurité sont frustrants ou difficiles à utiliser, les utilisatrices et utilisateurs pourraient les désactiver, les éviter ou les utiliser d'une manière qui va à l'encontre des exigences de sécurité et des besoins de protection pour lesquels les mécanismes ont été conçus.