CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

AC-20

Utilisation de systèmes externes

Juill. 2026

Votre gouvernement

Québec

AC

Gestion des droits d'accès aux systèmes et données

Access Control

AC-20 — Utilisation de systèmes externes (PaF-)

Énoncés :

a. [Sélection (un choix ou plus) : Établir les {Affectation : conditions générales d'utilisation définies par l'organisation}; identifier les {Affectation : contrôles définis par l'organisation dont la mise en place est présumée sur les systèmes externes}], conformément aux relations d'approbation établies avec les autres organisations qui possèdent, exploitent et/ou maintiennent les systèmes externes, de manière à ce que les personnes autorisées puissent faire ce qui suit :

1. accéder au système à partir des systèmes externes

2. traiter, stocker ou transmettre de l'information contrôlée par l'organisation au moyen de systèmes externes

b. Interdire l'utilisation de [Affectation : types de systèmes externes définis par l'organisation]

Paramètres :

a. assurer un niveau de sécurité équivalent aux actifs internes à l'organisation
b. système non conforme aux exigences de sécurité ou ciblé par une interdiction (ex.: indication d'application, attentes, orientations, etc.)

Responsable : OP

Discussion :

Par systèmes externes, on entend les systèmes qui sont utilisés par des systèmes organisationnels, sans en faire partie, et sur lesquels l'organisation n'exerce aucun contrôle direct sur le plan de la mise en oeuvre des contrôles requis ou de l'évaluation de l'efficacité des contrôles. Les systèmes externes comprennent les systèmes, les composants ou les appareils appartenant à des particuliers; les dispositifs de calcul et de communication appartenant à des intérêts privés dans des installations commerciales ou publiques; les systèmes appartenant à des organismes non gouvernementaux ou sous le contrôle de tels organismes; les systèmes gérés par des entrepreneures et entrepreneurs; et les systèmes d'information gouvernementaux qui ne sont ni la propriété des organisations, ni exploités ou contrôlés sous leur supervision directe et leur autorité. Les systèmes externes comprennent également les systèmes qui sont la propriété d'autres éléments de la même organisation (ou exploités par ces derniers) et les systèmes au sein de l'organisation dont les limites d'autorisation sont différentes. Les organisations ont l'option d'interdire l'utilisation de tous les types de systèmes externes ou de certains types de systèmes externes (par exemple, interdire l'utilisation de systèmes externes qui n'appartiennent pas à l'organisation ou interdire l'utilisation de systèmes appartenant à des particuliers). Dans le cas de certains systèmes externes (c'est-à-dire ceux exploités par d'autres organisations), les relations d'approbation établies entre ces organisations et l'organisation concernée peuvent être telles qu'aucune condition générale d'utilisation explicite n'est requise. Les systèmes dans ces organisations ne peuvent pas être considérés comme des systèmes externes. Ces situations se produisent, par exemple, lorsque des ententes d'échange d'information (implicites ou explicites) existaient déjà et avaient été établies entre les organisations ou composants, ou lorsque de telles ententes sont stipulées dans les lois, les décrets, les directives, la réglementation, les politiques ou les normes applicables. Les personnes autorisées comprennent notamment le personnel de l'organisation, les entrepreneures et entrepreneurs ou toute autre personne autorisée à accéder aux systèmes organisationnels et à qui les organisations sont en droit d'imposer des règles de conduite précises quant à l'accès au système. Les restrictions que les organisations imposent aux personnes autorisées n'ont pas besoin d'être uniformes puisqu'elles peuvent varier selon les relations de confiance entre les organisations. Par conséquent, les organisations peuvent choisir d'imposer aux entrepreneures et entrepreneurs des restrictions de sécurité différentes de celles imposées à un gouvernement fédéral, provincial ou municipal. Les systèmes externes utilisés pour accéder aux interfaces publiques qui mènent aux systèmes de l'organisation ne sont pas visés par le contrôle AC-

20. Les organisations établissent les conditions générales d'utilisation des systèmes externes conformément à leurs stratégies et procédures de sécurité. Au minimum, les conditions générales d'utilisation portent sur les types d'applications accessibles sur les systèmes organisationnels à partir des systèmes externes, et la catégorie de sécurité la plus élevée de l'information qui peut être traitée, stockée ou transmise dans des systèmes externes. Si les organisations ne peuvent pas établir des conditions générales d'utilisation avec les propriétaires des systèmes externes, elles peuvent imposer des restrictions au personnel utilisant ces systèmes externes.