Arrêté numéro 2023-02 du ministre de la Cybersécurité et du Numérique en date du 20 décembre 2023

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement
(chapitre G-1.03, a. 21)
Loi sur le ministère de la Cybersécurité et du Numérique
(chapitre M-17.1.1, a. 3 par. 8°)

CONCERNANT des exigences en matière de sécurité de l'information applicables aux organismes publics au regard de leurs actifs informationnels

---ooo0ooo---

LE MINISTRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE,

VU le deuxième alinéa de l'article 21 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03) suivant lequel le ministre de la Cybersécurité et du Numérique peut déterminer des orientations portant sur les principes ou les pratiques à appliquer en matière de gestion des ressources informationnelles, incluant les pratiques pour optimiser l'organisation du travail de même que la nécessité de considérer l'ensemble des technologies offrant un potentiel d'économies ou de bénéfices et des modèles de développement ou d'acquisition disponibles pour répondre aux besoins des organismes publics, dont les logiciels libres;

VU le paragraphe 8° de l'article 3 de de la Loi sur le ministère de la Cybersécurité et du Numérique (chapitre M-17.1.1) suivant lequel le ministre de la Cybersécurité et du Numérique assume les responsabilités d'établir des exigences en matière de sécurité de l'information applicables aux organismes publics et d'ordonner à ces derniers, lorsque requis, de mettre en œuvre ces exigences afin

d’assurer la protection de leurs actifs informationnels et des informations qu’ils supportent;

CONSIDÉRANT qu’il y a lieu, pour le ministre de la Cybersécurité et du Numérique, d’établir des exigences en matière de sécurité de l’information applicables aux organismes publics au regard de leurs actifs informationnels et d’ordonner la mise en œuvre de ces exigences afin d’assurer la protection de leurs actifs informationnels et des informations qu'ils supportent;

ARRÊTE CE QUI SUIT :

DÉTERMINE des orientations en matière de sécurité de l’information, soient celles déterminées dans les Exigences en matière de sécurité de l’information applicables aux organismes publics au regard de leurs actifs informationnels, annexées au présent arrêté;

ORDONNE aux organismes publics de mettre en œuvre de telles exigences afin d’assurer la protection de leurs actifs informationnels et des informations qu'ils supportent.

Québec, le 20 décembre 2023

Le ministre de la Cybersécurité et du Numérique,

ÉRIC CAIRE

ANNEXE
Exigences en matière de sécurité de l'information applicables aux organismes publics au regard de leurs actifs informationnels

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03, a. 21)
Loi sur le ministère de la Cybersécurité et du Numérique (chapitre M-17.1.1, a. 3 par. 8°)

1. Le ministre de la Cybersécurité et du Numérique établit, au moyen des présentes, des exigences en matière de sécurité de l'information applicables aux organismes publics au regard de leurs actifs informationnels.

2. Un organisme public doit, au regard de ses infrastructures et de ses systèmes, effectuer une évaluation des risques en fonction de l'utilisation qui est faite des équipements de vidéosurveillance et de télécommunication fabriqués par les sociétés suivantes, incluant celles qui y sont liées:

- Hangzhou Hikvision Digital Technology Co., Ltd.
- Zhejiang Dahua Technology Co., Ltd.

3. Un organisme public doit déployer les mesures de mitigations suivantes à l'égard des actifs informationnels utilisant des équipements visés à l'article 2 :

- Déployer les dernières mises à jour logicielles.
- Utiliser uniquement des équipements supportés par le manufacturier.
- Retirer tout appareil en fin de vie de son cycle de soutien logiciel.
- Utiliser un pare-feu, et effectuer de la surveillance des flux réseaux des appareils.
- Utiliser la segmentation pour isoler les appareils dans un segment réseau dédié.
- Ne pas exposer les appareils à Internet.
- Désactiver les fonctions non nécessaires au fonctionnement de la solution (ex. : géolocalisation).
- Changer le mot de passe administrateur par défaut du manufacturier par un mot de passe fort et utiliser l'authentification multifacteur lorsque disponible.
- Éviter de réutiliser des mots de passe sur plusieurs appareils.
- Restreindre l'accès physique aux appareils utilisés pour le stockage et le traitement des enregistrements.

4. Tout équipement visé à l'article 2, acquis après le 21 décembre 2023, ne peut être installé ou utilisé par un organisme public.