

## Gestion du système Artemis

### Mise en contexte

Pour répondre continuellement aux appels et à l'instar des corps de sapeurs-pompiers de plusieurs grandes villes canadiennes, le Centre de communication en sécurité incendie (CCSI) du Service de sécurité incendie de Montréal (SIM) utilise un système informatique de répartition des appels appelé Artemis depuis novembre 2007. Le SIM, qui compte 67 casernes, est l'unique corps de ce genre dans toute l'agglomération de Montréal à assurer la sécurité de la population montréalaise.

Ainsi, il est crucial pour lutter efficacement contre les incendies et répondre aux appels, que le SIM, plus précisément le CCSI, puisse s'appuyer sur un système performant avec une haute disponibilité visant à distribuer les appels entrants parmi les 2 739 membres du personnel du service. En 2022, ceux-ci ont pris en charge 118 916 interventions d'urgence incendie et à titre de premiers répondants dans la Ville de Montréal (la Ville).

### Objectif de l'audit

Déterminer si les mécanismes de contrôle en place permettent une saine gestion ainsi qu'une haute disponibilité du système Artemis du SIM.

### Résultats

Globalement, nous concluons que la Ville a mis en place plusieurs mécanismes de contrôle assurant une saine gestion du système Artemis. En effet, la définition des rôles et responsabilités, le processus de gestion des correctifs et des mises à jour, la surveillance des niveaux de services, les ressources humaines spécialisées, les comptes à haut privilèges et le plan de relève informatique sont adéquats.

Cependant, certains éléments nécessitent des améliorations, dont les paramètres d'authentification d'Artemis, la procédure sur la gestion des accès logiques à hauts privilèges, la documentation fonctionnelle de l'environnement du système d'Artemis et les mécanismes d'alertes automatisées pour les incidents.

## Principaux constats

### Gouvernance

- Les rôles et responsabilités des parties prenantes à la gouvernance et la gestion du système Artemis sont documentés.

### Gestion des accès logiques

- Aucun compte obsolète à hauts privilèges n'est présent dans Artémis.
- Le standard de la Ville sur la gestion des accès logiques qui décrit les exigences sur les paramètres d'authentification n'est pas appliqué à Artemis 2.6.
- Il n'existe pas de procédure de gestion des accès logiques à hauts privilèges pour Artemis, Smartemis et Artemis Web.

### Gestion des correctifs et des mises à jour

- L'implantation de la nouvelle version d'Artemis a été réalisée selon les meilleures pratiques. Cependant, ce processus n'est pas documenté dans une procédure.

### Gestion des incidents

- La procédure de gestion des incidents d'Artemis respecte les saines pratiques.
- Aucun mécanisme d'alertes automatisées n'est en place dans l'environnement Artemis. Cependant, le personnel du CCSI, étant présent en tout temps, détecterait en temps réel tout problème.

### Surveillance

- Des niveaux de services avec le fournisseur intégrateur sont définis et suivis lors des rencontres du comité de pilotage.

### Ressources spécialisées

- Le SIM et le Service des technologies de l'information (STI) comptent un nombre suffisant de ressources humaines spécialisées en soutien au maintien en conditions opérationnelles du système Artemis.

### Documentation fonctionnelle

- La documentation fonctionnelle d'Artemis n'est pas systématiquement mise à jour à chaque changement de son environnement.

### Relève informatique

- Un plan de relève informatique adéquat a été développé et fait l'objet de tests annuels.

En marge de ces résultats, nous avons formulé différentes recommandations aux unités d'affaires qui sont présentées aux pages suivantes.