Ville de Lausanne
Contrôle des finances
case postale 6904 – 1002 Lausanne

RAPPORT D'AUDIT INTERNE

Gestion des accès informatiques

Audit de Sécurité informatique

Destinataires :

Municipalité

Madame la Directrice du Logement, de l'environnement et de l'architecture

Madame la Cheffe du Service d'organisation et d'informatique

Extrait de la directive municipale sur le Contrôle des finances de la Ville de Lausanne[1]

Art. 18 – Rapports d'audit interne et recommandations

1. Le mandat d'audit débute par un entretien de lancement avec l'audité.
2. Le CFL émet le rapport en version définitive aux destinataires prévus uniquement après la finalisation des étapes suivantes :
   a. Le CFL présente ses conclusions d'audit et recommandations dans un projet de rapport qu'il adresse avant la réunion de clôture à l'audité.
   b. Lors de la réunion de clôture, l'audité fait part de ses éventuelles remarques sur les constats et recommandations du projet de rapport.
   c. A l'issue de cette réunion, le CFL émet une version du projet adressée à l'-aux audité-s et au-x directeurs concerné-s pour prise de position.
   d. L'audité a 60 jours ouvrés pour faire adopter une note à la Municipalité comprenant :
      i. sa position pour chaque recommandation. Si une recommandation s'adresse à un tiers, le CFL adresse séparément sa demande de positionnement à ce dernier ;
      ii. une note de synthèse de suivi des recommandations de l'audité ;
      iii. l'indication des éléments considérés comme étant confidentiels ainsi que les motifs afin que la Ville puisse en tenir compte lors de la publication du rapport.

      Lorsque l'audité n'est pas une entité rattachée à l'administration communale, le service de tutelle doit soumettre la note à la Municipalité, qui en prendra acte.
   e. Le délai de 60 jours écoulé, le CFL émet le rapport final aux destinataires prévus à l'art. 19 al. 1. Celui-ci inclut les prises de position et la note de synthèse de suivi des recommandations de l'audité.
3. En cas de désaccord au sujet des recommandations à mettre en œuvre, le CFL saisit le comité d'audit, qui statue définitivement.
4. Lorsque l'audité n'a pas donné, dans le délai imparti, une suite appropriée aux recommandations du CFL, celui-ci soumet le cas au comité d'audit qui prend les dispositions nécessaires.

Art. 19 - Diffusions des rapports

1. Les rapports d'audit interne sont adressés :
   a. A l'audité ;
   b. Au service subventionnant concerné, lorsque l'audité n'est pas une entité rattachée à l'administration communale ;
   c. A la direction concernée ;
   d. A la Municipalité ;
2. Sous réserve des dispositions de l'art. 16 LInfo, les rapports d'audit interne sont rendus publics dès qu'ils sont achevés au sens de l'article 9 alinéa 1er LInfo, soit dès que le rapport final a été émis par le CFL.
3. Les noms des collaborateurs ne sont pas mentionnés dans le rapport publié.

Remarque

« Les informations contenues dans le présent document (le « Document ») sont destinées aux seuls besoins internes de l'audité et de la Ville de Lausanne. L'utilisation directe ou indirecte par un tiers de tout ou partie du Document s'effectuera sous sa seule responsabilité. Le Document s'appuie sur les faits et circonstances bien particuliers tels qu'ils ont été présentés au Contrôle des finances au moment de sa rédaction et n'a pas vocation à valoir pour le futur. Les destinataires seront seuls compétents et responsables pour la mise en œuvre des recommandations. »

[1] Directive municipale sur le Contrôle des finances de la Ville de Lausanne du 14 janvier 2021 et entrée en vigueur le 14 janvier 2021 : Directive municipale sur le CFL

Synthèse

Le Service d'organisation et d'informatique assure le suivi, le développement et la maintenance du système d'information de la Ville de Lausanne ainsi que le support aux utilisateurs pour l'ensemble des collaborateurs. L'informatique est un domaine en constante et rapide évolution entrainant l'apparition de nouvelles technologies et donc de nouveaux enjeux liés à la sécurité.

Suite aux récents évènements de cybercriminalité opérés dans certaines communes et à la place prépondérante qu'occupe la sécurité dans le domaine informatique, le Service du contrôle des finances (CFL) a souhaité auditer la gestion des accès informatiques au sens large au sein de la Ville.

Le CFL s'est concentré sur trois domaines différents concernant la sécurité dont voici un bref résumé des actions recommandées :

- Les droits d'accès applicatifs, serveur de fichiers et physiques :
    - Rédiger une directive sur gestion des droits d'accès au serveur de fichier et droit d'accès applicatifs ;
    - Mettre à jour la base de données de gestion de configuration et créer son processus de mise à jour afin d'attribuer systématiquement un responsable, un groupe de validation et un prix pour chacune des solutions ;
    - Établir un référentiel contenant la liste des validateurs d'accès au serveur de fichiers et adapter son processus d'attribution des droits en fonction de ce référentiel ;
    - Assurer une continuité de l'activité de gestion des badges d'accès en formant une ressource à la suppléance et en capitalisant une procédure d'attribution et de suppression avec des responsables, des validateurs et des contrôles.
- Les processus liés aux mots de passe :
    - Appliquer opérationnellement la directive sur l'usage et la gestion des mots de passe en matière de rétention, de complexité et de durée ;
    - Modifier le processus de réinitialisation de mot de passe afin de garantir une cohérence entre la gouvernance et l'opérationnel et de prévoir les départs des collègues administrateurs du système d'information ;
    - Inspecter soigneusement et épurer la liste des comptes opérateurs en supprimant les comptes non légitimes et en séparant les droits par unité d'organisation.
- La gestion des comptes administrateurs, utilisateurs et de services :
    - Rédiger et mettre en place une directive sur la gestion des comptes ;
    - Finaliser le programme de sensibilisation et formation des utilisateurs à la sécurité informatique ;
    - Créer un processus transverse permettant aux ressources humaines et aux équipes techniques de formaliser les échanges sur les arrivées et départs de personnel ;
    - Traiter les différentes anomalies de sécurité liées aux comptes et trouvées lors de l'audit.

Sur la base de ses travaux, le CFL a formulé 11 recommandations permettant d'améliorer la sécurité du système d'information de la Ville sur le thème de la gestion des accès informatiques.

Tableau des recommandations

N°	Année	Sujet	Responsables	Risques	Priorité
R1	**2021**	Rédaction d'une politique de gestion des accès applicatifs et serveur de fichiers	SOI	Gouvernance	Elevée
R2	**2021**	Mise à jour de la base de données de configuration	SOI	Management Opérationnel	Moyenne
R3	**2021**	Référentiel des validateurs d'accès informatiques	SOI	Management	Elevée
R4	**2021**	Gestion des badges d'accès physiques	SOI	Gouvernance	Elevée
R5	**2021**	Application de la directive sur la gestion et la complexité des mots de passe	SOI	Opérationnel	Elevée
R6	**2021**	[redacted]	SOI	Opérationnel	Moyenne
R7	**2021**	Anomalies d'accès à la gestion des mots de passe	SOI	Management	Elevée
R8	**2021**	Programme de formation et sensibilisation à la sécurité informatique	SOI	Gouvernance	Moyenne
R9	**2021**	Publication de la directive sur la gestion des comptes informatiques	SOI	Gouvernance	Faible
R10	**2021**	Processus transverse d'arrivées et départs des collaborateurs	SOI SPeL	Gouvernance Management	Moyenne
R11	**2021**	[redacted]	SOI	Opérationnel	Elevée

SOI : Service d'organisation et d'informatique
SPeL : Service du Personnel

Note de synthèse du suivi des recommandations (élaborée par l'audité)

Prise de position générale (facultatif)

La gestion des accès et des identités (GDIA) est un pilier essentiel de la Sécurité de l'Information, qu'il convient de mettre en place afin de garantir un contrôle efficace des accès. La mise en place d'un tel processus à l'échelle de la Ville de Lausanne permettra de gérer le cycle de vie des identités, de provisionner les accès dans les différents systèmes et applications et de s'assurer que les droits d'accès sont correctement affectés et gérés.

Le Système d'Information de la Ville a évolué par opportunité, privilégiant la numérisation de processus métier au détriment de démarches transverses sans valeur ajoutée directe pour les utilisateurs.

Le Service d'organisation et d'informatique (SOI) recommande la mise en place d'un système de gestion des accès et des identités, avec les processus associés.

Commentaire général sur les prises de position sur les recommandations (facultatif)

Néant.

Etat du suivi des recommandations

Certaines des recommandations émises ont déjà été mises en œuvre ou seront prises en compte rapidement par le SOI. D'autres recommandations nécessitent un plus long travail de mise en œuvre et sont liées notamment à l'octroi de moyens financiers prévus au plan des investissements (préavis Sécurité). Elles ne pourront pas être effectives avant 2025, ou même 2027 en ce qui concerne le projet à réaliser en collaboration avec le Service du personnel.

Plusieurs mesures listées dans les recommandations sont des tâches et des actions effectuées et automatisées dans un système GDIA. Ces tâches sont chronophages si elles ne sont faites que manuellement, et devraient être effectuées en permanence.

Plusieurs autres mesures font partie intégrante du SMSI (Système de Management de la Sécurité de l'Information). Les politiques de sécurité définissent des cibles à atteindre, et des directives les accompagnent pour en définir/ordonner l'application. Des décalages peuvent être constatés entre la cible voulue et la situation à un instant T, ils sont traités en mode d'amélioration continue.

Par ailleurs, des mesures de correction et d'amélioration sont menées dans le cadre d'un projet de restructuration de l'annuaire interne. Elles concernent particulièrement les bonnes pratiques de gestion des comptes et des groupes, les processus de validation, etc.

Table des matières

1. Introduction

1.1 Préambule

Le contenu de ce rapport a fait l'objet d'une revue complète par l'audité avant la réunion de clôture le 23 février 2022. Les constats tels que repris dans ce rapport ont été validés lors de cette séance. Les recommandations, relevant quant à elles de l'opinion du CFL, ont été présentées et discutées avec l'audité.

A compter de la date d'émission du présent rapport dans sa version projet, l'audité disposera de 60 jours ouvrables pour prendre position sur les recommandations, élaborer la note de synthèse du suivi des recommandations et se déterminer sur la publication du rapport. A l'issue de ce délai, le rapport sera émis sous sa forme définitive et envoyé notamment à la Municipalité. Sous réserve des dispositions de l'art. 16 LInfo, le rapport d'audit interne sera rendu public.

Lettre de mission	4 août 2021
Réunion d'ouverture	19 juillet 2021
Remise du projet de rapport	3 février 2022
Réunion de clôture	23 février 2022
Rapport en version projet avant réponses de l'audité	8 juin 2022
Remise des réponses de l'audité aux recommandations	20 janvier 2023

Le CFL tient à remercier l'ensemble des collaborateurs du service pour leur disponibilité et leur coopération lors de nos travaux d'audit.

1.2 Contexte, terminologie et périmètre d'audit

Le Service d'organisation et d'informatique (SOI) est en charge de la surveillance, la maintenance, l'exploitation, et le développement de l'informatique de la Ville de Lausanne. Il assure également un service de veille informatique afin de se tenir au courant des dernières innovations.

Compte tenu de la rapidité à laquelle l'informatique évolue, le monde professionnel doit également s'adapter en sécurisant son système d'information afin de se prémunir, notamment, contre d'éventuelles cyber-attaques. En effet, les failles liées aux processus sans contrôles ou aux actes malveillants favorisent le piratage de données comme nous avons pu le voir récemment dans certaines communes vaudoises.

L'objectif de cet audit est multiple, le CFL a souhaité regarder si les politiques ou directives liées à la gouvernance, les processus dépendant du management et les actions réalisées opérationnellement sont sécurisés, bien définis, maitrisés et contrôlés afin de vérifier la sécurité du système d'information à tous les niveaux.

Les 3 grands thèmes couverts par l'audit sont les suivants :

- La gestion des accès :
    - Applicatifs : Comment sont mis en place, contrôlés et sécurisés les droits pour les logiciels ;
    - Réseaux : Comment les accès sur le serveur de fichiers sont attribués, modifiés et supprimés ;
    - Physiques : La gestion des badges d'accès physiques du SOI avec un focus sur les centres de données.
- Les mots de passe : La stratégie de complexité, sa mise en œuvre et le processus de réinitialisation
- Les comptes :
    - Administrateur : Les comptes permettant d'administrer le système d'information ;
    - Utilisateur : Les comptes de tous les collaborateurs de la Ville ;
    - Service : Les comptes spéciaux destinés aux applications, scripts et non autorisés à s'authentifier sur une session Windows.

Note : Sont exclus de cet audit les tests d'intrusions dans le réseau et l'analyse des équipements ou version de navigateurs et systèmes d'exploitation.

2. Les accès applicatifs, serveur de fichiers et physiques

2.1 Gouvernance

Dans sa configuration actuelle, le Service d'organisation et d'informatique (SOI) dispose d'une équipe de gouvernance qui assure plusieurs fonctions dont la gouvernance sécurité, la gestion des risques du système d'informations et rédige les politiques de sécurités associées. La sécurité opérationnelle est, elle, opérée au travers de chacune des équipes et sous la responsabilité des managers ou chefs de division.

Dans un principe de fonctionnement général, la gouvernance à le rôle de mettre en place des politiques ou directives puis de les communiquer aux équipes opérationnelles pour leur mise en place au travers de processus et d'outils techniques.

Le CFL constate qu'il n'existe pas à ce jour de politique ou directive régissant les règles fondamentales sur la gestion des accès informatiques applicatifs et serveur de fichiers. Ce périmètre est géré au quotidien par les équipes opérationnelles sans bénéficier d'une vision plus globale du système d'information.

R1. Rédaction d'une politique de gestion des accès applicatifs et serveur de fichiers

Le CFL recommande la mise en place d'une politique régissant l'attribution, la modification et la suppression de droits d'accès au serveur de fichier et aux applications pour les collaborateurs.

Le CFL recommande également la mise en place d'un référentiel exhaustif des validateurs habilités à délivrer une autorisation d'accès en phase avec les outils techniques.

Risque	Responsable	Priorité
Gouvernance	SOI	Elevée

Position de l'audité	Acceptée	~~Contestée~~	
Eléments clés de la mise en œuvre : Plusieurs éléments sont existants et présents dans des documents variés, mais ne couvrent pas l'ensemble de la problématique. De plus, des bonnes pratiques sont en place avec la gestion des droits d'accès via des groupes. La mise en place d'une telle politique doit se faire à travers un système de gestion des identités et des accès. Le deuxième point est redondant avec un point de la R3.			
Personne responsable de la recommandation	[redacted]	**Délai**	31.12.2023

2.2 La gestion des accès applicatifs

Au sein du SOI, une distinction est faite entre un logiciel, qui est une solution achetée et installée sans trop de personnalisation et les applications, qui sont des solutions soit achetées et personnalisées soit développées spécifiquement pour les besoins métiers de la Ville.

Plusieurs acteurs et processus interviennent dans la gestion des accès applicatifs. La demande doit passer par un ticket sur la solution Easyvista qui enclenche le processus opérationnel. Selon le logiciel ou les accès demandés, le processus et donc les acteurs seront différents. Par exemple, si le logiciel est payant, il nécessitera une validation du service achat et du management mais s'il est gratuit, ces étapes de validation ne seront pas nécessaires. Pour une application métier, la validation se fera du côté métier dans le service concerné.

La base de données de gestion de configuration contenue dans l'outil d'inventaire Easyvista recense la carte d'identité de chacune des applications et logiciels, permettant de savoir quel processus sera utilisé. Il est donc primordial que cette base de données soit à jour et exhaustive.

A travers ses travaux d'audit, le CFL a identifié des incohérences dans la base de données ainsi que des champs non renseignés pour plusieurs logiciels ou applications comme l'absence de prix ou de responsable applicatif. Cette absence se justifie entre autre par le manque de personnel dédié à la gestion de ces

applications métiers ainsi qu'un manque de rationalisation des applications. Le contexte particulier de la Ville de Lausanne implique plusieurs cœurs de métiers et cette multitude d'activités implique elle-même une multitude d'applications pour y répondre.

Un logiciel payant renseigné comme gratuit pourrait par exemple être installé par les équipes techniques sans faire l'objet d'un achat de licence ni même d'une validation hiérarchique.

De plus, pour trois applications critiques ayant été décortiquées, le CFL a constaté une absence de contrôle des groupes d'accès. Le processus d'attribution et de validation fonctionne correctement, cependant, pour certaines applications transverses à plusieurs services, il n'existe pas de lien dans le processus de suppression ou dans les contrôles des droits entre les équipes techniques du SOI et les équipes métiers.

Pour être plus précis, l'attribution des droits dans les applications métiers est bien validée mais il n'existe pas de contrôles à posteriori. Par ailleurs, aucun contrôle n'est effectué en relation avec l'autorisation d'accès via les groupes Active Directory (AD), qui permettent l'installation ou l'octroi de droits applicatifs.

De plus, le CFL a constaté une absence de responsable sur la liste des collaborateurs présents dans les groupes AD, les services métiers rejetant la responsabilité sur le SOI et inversement.

R2. Mise à jour de la base de données de configuration

Le CFL recommande de mettre à jour la base de données de gestion de configuration afin :

- D'attribuer un responsable produit pour chacune des solutions dans le logiciel d'inventaire Easyvista ;
- D'attribuer un groupe de validation pour les 46 applications orphelines ;
- De définir un responsable en charge du contrôle régulier des groupes d'accès applicatifs dans l'Active Directory et automatiser sa mise en place ;
- De renseigner le prix de toutes les applications afin que les payantes passent par un workflow de validation.

Risque	Responsable	Priorité
Management Opérationnel	SOI	Moyenne

Position de l'audité	Acceptée	~~Contestée~~	
Eléments clés de la mise en œuvre : C'est une mise à jour des inventaires d'application et de solutions à effectuer dans l'outil de gestion des services IT.			
Personne responsable de la recommandation	[redacted]	**Délai**	31.12.2023

2.3 La gestion des accès au serveur de fichiers

La gestion des accès au serveur de fichiers se fait par l'AD, un système d'annuaire et de gestion de l'identification et de l'authentification. Il permet entre autre d'attribuer des droits en lecture ou écriture sur un dossier sur le serveur de fichiers.

La gestion des droits d'accès, par bonnes pratiques, se fait par des groupes afin de pouvoir gérer plus facilement les utilisateurs et les accès.

Lors de notre audit, nous nous sommes heurtés à des difficultés concernant l'identification des personnes responsables des accès sur les serveurs. En effet d'une part, il n'existe pas de workflow permettant d'alerter lorsqu'un validateur est absent, malade ou quitte la Ville. D'autre part, ces personnes sont désignées arbitrairement et ne possèdent pas forcément ces attributions dans leur description de poste.

Nous avons également trouvé des centaines de groupes vides, n'ayant aucune utilité, polluant ainsi l'outil Active Directory et ralentissant la mise en œuvre par les collaborateurs actuels.

Enfin, aucun contrôle régulier et planifié de ces groupes n'existe auprès des responsables de ces groupes ni auprès du SOI. Ces contrôles sont nécessaires afin de s'assurer que le départ d'un collaborateur ou le changement d'équipe d'un collaborateur a bien été effectué et que celui-ci possède à l'instant T les droits adéquats sur le serveur de fichiers.

Nous relevons également qu'un point de vigilance doit être apporté sur les comptes des personnes à responsabilités qui ont souvent trop de droits au vue de leur faible activité opérationnelle. Par exemple sur les comptes administrateurs, peu nombreux mais à forts pouvoirs, ainsi que les comptes stagiaires ou apprentis qui cumulent parfois les droits de plusieurs équipes lors de leur formation ou apprentissage.

Le CFL constate que l'outil d'audit des accès au serveur de fichiers permet la mise en place d'alertes automatiques de sécurité. Il mérite d'être peaufiné afin d'intégrer ces alertes permettant de détecter en temps réel les potentielles failles de sécurité ou comportements suspects sur le serveur de fichier.

R3. Référentiel des validateurs d'accès informatiques

Dans le but d'améliorer la sécurité des accès au serveur de fichiers accordés aux utilisateurs, le CFL recommande de :

- Créer un référentiel listant tous les validateurs potentiels pour chacun des accès possibles ou de renseigner un responsable pour l'intégralité des groupes d'accès au serveur de fichiers ;
- Modifier le processus d'attribution d'accès au serveur de fichiers en intégrant ces responsables lors de l'étape de validation ;
- Supprimer les groupes vides n'ayant aucune utilité ;
- Définir une liste de contrôles à mettre en place sur un échantillon de droits accordés dans une procédure d'exécution avec un responsable d'action et une planification régulière, formalisée et automatisée dans la mesure du possible.

Risque	Responsable	Priorité
Management	SOI	Elevée

Position de l'audité	Acceptée partiellement	~~Contestée~~	
Eléments clés de la mise en œuvre : • L'affectation des droits au niveau du service de fichiers est déjà réalisée dans le mode préconisé, à savoir la validation d'un responsable de service. • L'attribution des droits est l'application d'une politique de gestion des identités et des accès qui doit se faire dans un système de gestion des accès et des identités. • Les groupes vides sont nécessaires pour certaines applications. Les groupes vides non nécessaires seront supprimés.			
Personne responsable de la recommandation	[redacted]	**Délai**	31.12.2023

2.4 La gestion des accès physiques au SOI

La gestion des accès physiques peut se faire par clés, badges, ou autre et permet une première barrière de sécurité afin de dissuader d'éventuels malfaiteurs. Cette gestion des accès doit être contrôlée, encadrée et sécurisée afin de pouvoir identifier toutes les personnes en capacité d'accéder aux locaux les plus critiques.

Au SOI, une personne est actuellement en charge, lors de l'arrivée d'un collaborateur du SOI, de faire remplir un formulaire, le contrôler, valider sa légitimité puis créer le badge d'accès associé. Cette personne ne bénéficie pas de suppléance depuis plusieurs mois et prendra prochainement sa retraite. Le CFL recommande au SOI d'anticiper la formation d'une nouvelle personne ou équipe et d'une suppléance sur cette activité.

Nous avons également trouvé des badges d'accès attribués non nominativement, ne permettant donc pas d'identifier la personne ayant utilisé cet accès. Le nom du responsable devrait figurer pour chacun des badges d'accès créés et attribués afin d'en responsabiliser le demandeur.

R4. Gestion des badges d'accès physiques

Afin d'assurer une continuité de l'activité de gestion des badges au sein du Service d'Organisation et d'Informatique, le CFL recommande de :

- Former une personne à la suppléance de la gestion des badges d'accès ou confier l'activité à une autre équipe, comme le helpdesk, déjà en charge de plusieurs actions du même type lors de l'arrivée de personnel ;
- Rédiger des procédures et processus permettant de traiter la gestion des collaborateurs à leur arrivée ou à leur départ en collaboration avec l'équipe des ressources humaines ;
- Renseigner le nom et le prénom des responsables pour chacun des accès donnés ;
- Supprimer les accès des 6 badges non nominatifs ;
- Mettre en place des contrôles réguliers et aléatoires sur les accès donnés.

Risque	Responsable	Priorité
Gouvernance	SOI	Elevée

Position de l'audité	Acceptée partiellement	~~Contestée~~	
Eléments clés de la mise en œuvre : • La suppléance pour la gestion des badges est déjà organisée suite au départ du titulaire précédent. • Les badges non nominatifs sont destinés à des utilisateurs occasionnels (1 à 5 jours), sous la responsabilité des chefs de pôle. • Il convient de formaliser les procédures d'arrivées et départ, qui sont normalement mis en œuvre dans le cadre d'une gestion des identités et des accès (GDIA).			
Personne responsable de la recommandation	[redacted]	**Délai**	31.12.2023

3. Les mots de passe

3.1 Directive sur la gestion et la complexité des mots de passe

La directive sur la gestion et la complexité des mots de passe régit plusieurs aspects sécuritaires dont notamment :

- L'interdiction d'enregistrer les mots de passe afin de faciliter l'authentification mettant ainsi la complexité du mot de passe de côté et rejetant la sécurité sur le système de sauvegarde du mot de passe ;
- La complexité des mots de passe et la nécessité de l'utilisation de symboles, majuscules, chiffres, longueur, etc… Une complexité non défini ou non appliqué favorise l'apparition de mots de passe génériques, standards et donc à faible niveau de sécurité ;
- La période de renouvellement des mots passe, initialement défini à 3 mois puis 9 pour la pandémie. Ayant retrouvé un rythme moins dans l'urgence, le CFL recommande de rétablir la période de renouvellement initiale de 3 mois ;
- La tenue et mise à jour d'un registre des dérogations liées à la sécurité comprenant toutes les mesures d'exceptions prises, contrevenant à la politique de sécurité du SI ;
- Le stockage sur papier ou matériel informatique sécurisé et hors réseau sous séquestre des mots de passe essentiels au bon fonctionnement du SI.

Des corrections ont été effectuées durant l'audit suite au caractère urgent de la situation sécuritaire du système d'information, que ce soit sur l'application de la politique de sécurité, sur les mots de passe ou sur les comptes.

Le CFL a également constaté que sur les 30 comptes de service testés, aucun ne respecte le critère de longueur de 20 caractères comme défini dans la directive sur la gestion et la complexité des mots de passe. La moyenne de longueur des mots de passe est de 11 caractères.

R5. Application de la directive sur la gestion et la complexité des mots de passe

Le CFL recommande d'appliquer la directive sur l'usage et la gestion des mots de passe afin de garantir :

- Une impossibilité de stocker les mots de passe dans les différents logiciels et navigateurs ;
- Une adéquation entre la politique de complexité des mots de passe configurée dans les outils informatiques et la directive sur la gestion des mots de passe ;
- Un rétablissement de la durée initiale de réinitialisation des mots de passe à 3 mois ;
- La tenue et mise à jour d'un registre des dérogations liées à la sécurité et maintenue par le Responsable de la Sécurité du Système d'Information comme mentionné dans cette même directive ;
- Une longueur minimale de 20 caractères pour tous les comptes de services ;
- La rédaction sur papier ou matériel informatique sécurisé et hors réseau, de la liste des mots de passe essentiels à l'administration de la Ville de Lausanne et une conservation sous séquestre dans un espace sécurisé.

Risque	Responsable	Priorité
Opérationnel	SOI	Elevée

Position de l'audité	Acceptée	~~Contestée~~	
Eléments clés de la mise en œuvre : • Une mise en cohérence entre la directive relative aux mots de passe et les pratiques est nécessaire, mais a un impact important sur la gestion des applications. A noter que la politique est une cible, son existence n'implique pas qu'une mise en conformité immédiate soit possible. • La durée des mots de passe à trois mois est rétablie. • Les mots de passe essentiels sont déjà sauvegardés sur un support physique hors ligne.			
Personne responsable de la recommandation	[redacted]	**Délai**	31.12.2023

[redacted]

- [redacted] ;
- [redacted] ;
- [redacted].

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

<table>
<tr><td>[redacted]</td><td>[redacted]</td><td colspan="2">[redacted]</td></tr>
<tr><td colspan="4">[redacted] :
[redacted]x.
[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td></tr>
</table>

3.3 Contrôle de conformité des administrateurs

Certains collaborateurs de la Ville possèdent un compte dit « Account Operator », c'est-à-dire qu'ils ont un droit particulier leur permettant de réinitialiser le mot de passe d'un autre collaborateur.

Le CFL a identifié plusieurs incohérences durant l'audit, impliquant nombre de failles de sécurité dans le SI.

Premièrement, plusieurs comptes non légitimes possèdent ce droit « Account Operator ». Ce droit est censé être réservé à certaines personnes qualifiées informatiquement et dont la description de poste autorise à procéder à cette réinitialisation de mot de passe.

Deuxièmement, plusieurs doublons ont été trouvés, rendant difficile l'exercice d'identification des administrateurs. Il existe à ce jour 103 « Account Operator » (avec les doublons), un chiffre plus élevés que les membres légitimes trouvés sur l'organigramme du service.

Ensuite, des comptes administrateurs de type « P_ » ont été trouvés dans la liste des compte dit « Account Operator ». Ce type de compte est pourtant défini comme administrateur d'un ou plusieurs postes de travail et ne devrait pas être autorisé à réinitialiser des mots de passe.

Enfin, des comptes hors SOI ont été identifiés, permettant à des collaborateurs du Corps de police, par exemple, de réinitialiser le mot de passe de n'importe quel collaborateur de la Ville. Le CFL constate qu'un cloisonnement des droits est possible mais n'a pas été mis en place, engendrant une faille supplémentaire de sécurité.

R7. <u>Anomalies d'accès à la gestion des mots de passe</u>

Le CFL recommande d'effectuer un nettoyage des comptes « Account Operator » pouvant réinitialiser les mots de passe des collaborateurs afin de :

- Supprimer les comptes des responsables d'équipe n'ayant aucune action opérationnelle et donc aucune légitimité à avoir ces accès ;
- Supprimer les doublons entre les comptes utilisateurs et administrateurs, notamment pour le centre de services informatique ;
- Supprimer les comptes utilisateurs ou administrateurs de poste de type « P_ ». Seuls les comptes de type « A_ » sont autorisés à être dans ce groupe d'accès ;
- Renseigner le champ description pour chacune des demandes afin d'en tracer les validations associées ;

- Mettre en place une séparation hiérarchique par Unité d'Organisation afin que les comptes hors SOI ne puissent réinitialiser les mots de passe que de leurs entités respectives ;
- Définir des contrôles périodiques et formalisés permettant de s'assurer du bon contenu des groupes administrateurs.

Risque	**Responsable**	**Priorité**
Management	SOI	Elevée

Position de l'audité	Acceptée	~~Contestée~~	
Eléments clés de la mise en œuvre : L'ensemble des points listés dans cette recommandation est pris en compte dans le cadre de la restructuration de l'Active Directory. Plusieurs points sont déjà réalisés ou en cours de réalisation.			
Personne responsable de la recommandation	[redacted]	**Délai**	31.12.2023

4. Les comptes administrateurs, utilisateurs et de service

4.1 Programme de formation et sensibilisation

Le SOI est actuellement la seule entité de la Ville à disposer des compétences et de la légitimité en matière de sécurité informatique et de prévention à la cybercriminalité. Par ailleurs, la grande majorité des collaborateurs de la Ville utilisent un ordinateur et la grande majorité des cas de piratage sont dus à des failles ou erreurs humaines. C'est pourquoi le CFL a analysé la gouvernance en place en matière de prévention et sensibilisation à la cybercriminalité.

Il existe un site d'e-learning permettant d'effectuer une autoformation et une autosensibilisation sur ce domaine mais cela reste facultatif, réalisé en 10 minutes environ par module. Cette formation, à l'arrivée du collaborateur, peut être demandée par le manager mais cela n'est pas systématique. De plus, cette formation est dispensée par l'équipe support informatique n'ayant pas reçu de formation particulière à la sécurité informatique.

Il n'existe pas à ce jour de programme de formation ou de sensibilisation des collaborateurs sur le sujet de la sécurité informatique. Certains services ont pris les devants et proposent, en interne, une autoformation et une sensibilisation mais le SOI est la seule entité compétente sur le sujet, elle devrait donc disposer d'une ressource à part entière dédiée à cette activité, notamment lors de l'accueil du collaborateur et de la remise de son poste de travail.

Un programme de sensibilisation est en cours de rédaction puis validation et diffusion. Nous avons reçu une ébauche de celui-ci. Nous encourageons cette démarche et attendons grandement sa mise en place. Nous constatons également que cela fait plusieurs années qu'aucune campagne de sensibilisation au hameçonnage n'a été effectuée.

R8. Programme de formation et de sensibilisation à la sécurité informatique

Dans le but d'améliorer la sécurité du système d'information et le niveau de compétence et de formation des collaborateurs de la Ville, le CFL recommande de :

- Créer un programme de formation et sensibilisation à la sécurité informatique pour tous les collaborateurs de la Ville de Lausanne ;
- Renforcer la formation à la sécurité informatique du centre de service informatique afin de pouvoir dispenser une formation de qualité aux nouveaux collaborateurs ;
- Reprendre les campagnes de sensibilisation au hameçonnage ;
- Dispenser la formation à l'ensemble des collaborateurs arrivant à la Ville.

Risque	Responsable	Priorité
Gouvernance	SOI	Moyenne

Position de l'audité	Acceptée	~~Contestée~~	
Eléments clés de la mise en œuvre : • Cette recommandation est acceptée mais est bien plus générale que la seule gestion des accès informatiques. • Un programme de sensibilisation est en ligne et disponible pour tous les utilisateurs. • Un nouveau programme de formation et de sensibilisation à la sécurité a été mis au point et sera déployé dès l'obtention des moyens financiers prévus au plan des investissements (Préavis Sécurité).			
Personne responsable de la recommandation	[redacted]	**Délai**	31.12.2025

4.2 Directive sur la gestion des comptes

Une directive sur la gestion des comptes des collaborateurs permet de régir les différents usages et modalités de gestion des comptes. Cela passe par la création, la modification et la suppression en assurant un cycle de vie complet des identités numériques.

Au niveau de la gouvernance, une directive a été transmise au CFL mais n'a jamais publiée. Sans version définitive et publiée, sur laquelle les équipes opérationnelles et managériales peuvent se reposer, il existe un risque de non cohérence et de violation des principes de sécurité liés à la création de compte.

Au niveau des processus, le CFL constate un manque de contrôles réguliers en place sur les comptes créés ou un suivi d'une toute autre action effectuée sur les comptes ainsi qu'une absence de processus spécifique pour la création de comptes non utilisateurs (services, techniques, etc…).

La directive de sécurité imposant des normes différentes pour certains types de comptes, on comprend que cette directive ne peut être correctement appliquée si aucun processus n'est dédié à la création de ces comptes spécifiques, réduisant la sécurité de ces derniers.

R9. Publication de la directive sur la gestion des comptes informatiques

Afin d'améliorer la gestion des comptes et de renforcer la sécurité du système d'information, le CFL recommande de :

- Rédiger en version définitive, une directive sur la gestion des comptes informatiques ;
- Mettre en place des contrôles réguliers, et si possible automatisés, des comptes créés, modifiés et supprimés ;
- Établir un processus et une procédure de création de compte spécifique aux comptes non utilisateurs.

Risque	**Responsable**	**Priorité**
Gouvernance	SOI	Faible

Position de l'audité	Acceptée partiellement	~~Contestée~~	
Eléments clés de la mise en œuvre : • La directive sur la gestion des comptes informatiques a été publiée. • Les processus de mise en œuvre et de contrôle sont en cours de mise en place, et sont en outre des tâches adressées dans une GDIA.			
Personne responsable de la recommandation	[redacted]	**Délai**	31.12.2023

4.3 Processus de création et suppression des comptes

4.3.1 Ressources humaines et équipes techniques

Le CFL a rencontré de grandes difficultés à reconstituer le processus d'arrivée de collaborateur car il n'existe à ce jour aucun processus transverse officiel.

Ce manque de clarté se traduit par des retards de traitement et la multiplication de tickets et d'échanges entre les collaborateurs. Un tel manque d'efficience doit rapidement être corrigé en organisant un processus commun avec l'intégralité des parties prenantes. Le CFL voit en cet exercice une opportunité de digitaliser le processus au maximum. En effet, le processus est digitalisé uniquement lors de la phase de création du ticket d'arrivée de personnel, par ailleurs incomplet car il n'inclut pas l'ensemble des besoins du collaborateur, forçant les managers à s'adresser à d'autres interlocuteurs.

Le processus actuel de gestion des comptes utilisateurs ne permet pas aux équipes techniques du SOI d'obtenir les informations adéquates provenant des services. Cela entrave le bon accomplissement de leur mission en matière de gestion des arrivées et départs de personnel.

La collaboration doit être renforcée entre les managers dans les services en charge de l'arrivée des prestataires externes, les ressources humaines dans les services, le service du personnel et le SOI afin d'améliorer la gestion des entrées et sorties de collaborateurs. La mutualisation d'une solution unique au travers d'un processus transverse unique entre les services est la clé de la réussite de la gestion des arrivées, transferts et sorties de collaborateurs. Des lacunes dans le processus et des manques de validations ont été constatés, notamment en la qualité du demandeur ou lors de demandes multiples.

Enfin, le CFL constate une absence de contrôles planifiés et réguliers permettant d'analyser un échantillon des dernières arrivées de personnel et ainsi procéder à une double vérification ainsi qu'une amélioration continue du processus d'arrivée ou de départ.

R10. Processus transverse d'arrivées et départs des collaborateurs

Le CFL recommande la mise en place d'un processus digitalisé de gestion des entrées et sorties du personnel en collaboration avec les ressources humaines et les équipes techniques en charge de la création et suppression des comptes.

Le processus d'arrivée d'un nouveau collaborateur devrait être initialisé ou validé par une personne légitime tel un manager ou un responsable. De la même manière, lorsque le collaborateur nécessite un compte administrateur supplémentaire, la demande doit être effectuée dans un ticket distinct passant par une validation des acteurs concernés.

Le CFL a constaté une absence de contrôles en place et recommande donc la mise en œuvre de contrôles planifiés, formalisés et réguliers sur les anomalies possibles liées aux comptes (expiration, départ, doublons, comptes administrateurs, etc…)

Risque	Responsable	Priorité
Gouvernance Management	SOI SPeL	Moyenne

Position de l'audité	Acceptée	~~Contestée~~	
Eléments clés de la mise en œuvre : Cette recommandation doit être traitée dans le cadre de la mise en place d'un système de gestion des accès et des identités. Un projet doit être initié en collaboration avec le Service du personnel.			
Personne responsable de la recommandation	[redacted]	**Délai**	31.12.2027

4.4 Anomalies de sécurité liées aux comptes non légitimes

Dans le cadre de l'audit, le CFL a effectué une analyse afin d'identifier des incohérences souvent présentes dans les SI et créant des failles de sécurité.

Ces incohérences sont souvent liées à des erreurs dans la robustesse des processus ainsi qu'à des erreurs humaines liées à la répétition des actions.

Il a ainsi été croisé, les informations venant de la base de données du personnel PeopleSoft avec la base de données technique de l'Active Directory, base de données utilisée entre autre pour la sécurité, les droits d'accès et l'authentification des utilisateurs.

Sur la base des anomalies de sécurité identifiées, le CFL a formulé la recommandation ci-dessous.

[redacted]

[redacted]

- [redacted];

- [redacted];
- [redacted];
- [redacted];
- [redacted].

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	
[redacted] - [redacted]. - [redacted]. - [redacted]			
[redacted]	[redacted]	[redacted]	[redacted]

Compte tenu des remarques et recommandations figurant dans le corps du présent rapport, et tout en formulant les réserves d'usage pour le cas où des documents, des renseignements ou des faits susceptibles de modifier nos considérations n'auraient pas été portés à notre connaissance au cours de nos travaux, cet audit n'appelle pas d'autre commentaire de notre part.

Lausanne, le 7 février 2023

Contrôle des finances de la Ville de Lausanne

Yves Tritten

2023-02-07 17:35

Signé électroniquement par Yves Tritten

Yves Tritten

Chef de service