Ville de Lausanne
Municipalité

Logement, environnement et architecture
Service d'organisation et d'informatique

Pilotage de la sécurité des systèmes d'information et de la protection des données pour la période 2023-2026

Demande de crédit d'investissement

Préavis Nº 2023 / 47

Lausanne, le 28 septembre 2023

Monsieur le Président, Mesdames, Messieurs,

1. Résumé

La Municipalité de Lausanne sollicite, par voie de préavis au Conseil communal, l'octroi d'un crédit de CHF 2'420'000.- destiné à financer le pilotage de la sécurité des systèmes d'information et de la protection des données sur une période de quatre ans (2023-2026). Le montant du présent préavis est revu pour couvrir le périmètre additionnel de protection des données et mener plus rapidement les changements majeurs dans un contexte international devenu plus risqué.

Le crédit d'investissement accordé en 2016 par le préavis N° 2015/73 « Renforcement de la sécurité des Systèmes d'Information pour la période 2016-2019 » a permis d'améliorer les protections existantes, de poser une politique de sécurité adaptée aux enjeux de la Ville et de mettre en place une démarche basée sur l'analyse des risques.

Les actions menées jusqu'ici ont permis de gagner en maturité dans beaucoup de domaines et il est nécessaire de poursuivre les efforts engagés pour traiter les risques et disposer d'un système d'information le mieux sécurisé possible. L'actualité récente montre qu'en Suisse, les administrations publiques sont ciblées par des attaques de pirates.

Le préavis pour la période 2023-2026 prévoit les axes de travail suivants :

1. gestion coordonnée des incidents de sécurité ;
2. gestion des identités et des accès ;
3. sensibilisation et formation à la sécurité de l'information ;
4. contrôle de la conformité et de l'efficacité ;
5. renforcement des socles techniques ;
6. sécurité des systèmes d'information industriels ;
7. protection des données.

Le présent préavis participe à la mise en œuvre de l'objectif suivant du programme de législature :

13. L'innovation pour faciliter la vie de toute la population.

2. Objet du préavis

Par le présent préavis, la Municipalité sollicite l'octroi d'un crédit d'investissement du patrimoine administratif de CHF 2'420'000.- afin de poursuivre les efforts de sécurisation et de gouvernance de la sécurité du système d'information (SI) et mettre en place une démarche de mise en conformité à la protection des données personnelles, et cela pour les années 2023 à 2026.

Les activités et projets présentés dans ce préavis visent à supporter un développement cohérent et durable du SI de la Ville tout en gardant sous contrôle les risques inhérents à son usage.

3. Préambule

L'échange d'informations est au cœur des métiers exercés au sein de l'administration communale lausannoise. Chaque jour, la Ville acquière, stocke, traite ou échange des informations. Très souvent, ces informations sont des données personnelles relatives à des personnes physiques : habitantes et habitants, clientes et clients, membres du personnel, partenaires/mandataires et bien d'autres.

Pendant des décennies, le traitement de ces informations a principalement été réalisé sous forme orale (par exemple aux guichets « usagers ») ou sous forme papier. Néanmoins, depuis plusieurs années, ces traitements sont majoritairement réalisés dans différentes solutions informatiques sous la forme de données numériques. Ces solutions constituent le Système d'information (SI) de la Ville.

Malheureusement, bien que les technologies numériques soient une incontestable source d'opportunités et de création de valeur, avec elles se développent de nouvelles menaces, nombreuses et complexes. Les organisations et les individus malveillants ont parfaitement compris les opportunités que leur offre ce nouvel espace et redoublent d'ingéniosité pour parvenir à leurs fins : sabotage, manipulations, propagande, fraudes, escroqueries, etc. Qu'il s'agisse d'individus isolés ou de groupes organisés, ces attaquants exploitent toutes les possibilités offertes.

Dans le même temps, la Ville se doit de respecter, en tant qu'administration publique et partenaire de confiance, la législation sur la protection des données. Plus que la protection de l'information en elle-même, il est principalement question de protéger l'identité et la vie privée des personnes concernées, mais aussi de préserver la confiance qu'elles placent en les services communaux.

Face à la réalité de cette transformation digitale, la Ville doit donc prendre en compte deux faits majeurs :

1. comme la majorité des organisations publiques ou privées, la Ville est et sera régulièrement confrontée à des problèmes de sécurité de l'information pouvant avoir un impact direct sur ses activités et sur la qualité des services rendus aux usagères et aux usagers ;
2. le législateur, que ce soit au niveau cantonal ou fédéral, prend petit à petit en compte la généralisation des technologies de l'information dans la société et renforce, d'une part, les exigences légales dans de nombreux domaines liés à la sécurité et à la protection des données, et d'autre part, ses activités de contrôle visant à évaluer les niveaux de risque encourus.

Dans ce monde numérique, tout incident de sécurité et toute non-conformité avec la législation peut ainsi avoir des conséquences significatives pour la Commune : interruption des services rendus, surcoûts, atteintes à l'image de marque, contentieux juridiques, atteintes à l'intégrité physique des personnes ou à leur personnalité, etc. Ces conséquences potentielles constituent un risque numérique que la Ville doit traiter. En conséquence, la sécurisation du Système d'information (SI) de la Ville et sa mise en conformité avec les exigences légales en matière de protection des données ne sont plus des options mais des prérequis.

4. Etat des lieux

4.1 Contexte

4.1.1 Sécurité de l'information

Depuis de nombreuses années, la Ville de Lausanne s'efforce de prendre en compte dans toutes ses démarches et activités la réalité du risque numérique. Cette prise en compte est

continue et incrémentale, et ne fait pas systématiquement l'objet de projets ou de plans d'actions spécifiques. Elle se base notamment sur les deux grands principes suivants :

1. principe d'amélioration continue : la Ville audite régulièrement les processus et les dispositifs techniques permettant d'assurer la sécurité, puis s'efforce d'améliorer le dispositif global ;
2. principe de la sécurité par conception : la Ville s'efforce de prendre en compte, dès la conception des solutions informatiques, puis tout au long de leur cycle de vie, les exigences de sécurité.

A ce jour, la Commune a déployé un ensemble de mesures organisationnelles et techniques visant à assurer la protection de son SI. La liste des mesures d'ores et déjà déployées comporte notamment :

- un dispositif de gouvernance permettant d'évaluer la situation, d'établir des règles de sécurité en fonction des risques réels et de contrôler leur mise en œuvre et leur efficacité ;
- un ensemble de mesures, techniques et organisationnelles, permettant une meilleure protection contre les incidents de sécurité ;
- une organisation humaine comprenant un responsable de la sécurité de l'information officiellement nommé, et un renforcement des compétences dans les différentes activités. Cependant, le maintien et le renforcement de ces mesures de sécurité est plus que jamais d'actualité, notamment du fait de l'augmentation constante des cybermenaces. L'actualité récente démontre que la criminalité numérique s'est intensifiée et que les organisations et les individus malveillants se sont organisés et professionnalisés. Quelques cas survenus durant ces cinq dernières années, notamment en Suisse, sont illustrés en annexe 1. Les attaques dont la Ville de Lausanne a fait l'objet pendant cette période sont également listées en annexe 2.

4.1.2 Sécurité de l'informatique industrielle

Pour la Ville, le risque numérique est d'autant plus élevé que ses services exploitent et pilotent, à l'aide de systèmes informatiques, plusieurs procédés industriels essentiels à la population :

- production, transport et distribution d'électricité ;
- production et distribution d'eau potable ;
- traitement des eaux usées ;
- transport et distribution de gaz naturel ;
- production et distribution de vapeur d'eau à haute température pour le chauffage à distance.

Plusieurs éléments contribuent à l'augmentation du risque numérique pour ces installations :

- les services concernés utilisent des dispositifs techniques (par exemple les automates industriels) intégrant systématiquement des composants informatiques ;
- les services concernés interconnectent leurs systèmes industriels au SI de gestion, notamment pour faciliter et accélérer la facturation des services ;
- les services concernés sous-traitent certaines opérations en donnant accès à des tiers externes à leurs systèmes industriels ;
- la prise en compte de la sécurité par le monde industriel est récente (3 à 7 ans en Suisse) et doit encore progresser partout, y compris dans les services de la Ville.

Il est important de noter que la transformation numérique des SI industriels est une démarche normale, commune à toutes les industries. Néanmoins, l'augmentation constante

des risques et le renforcement des exigences réglementaires imposent à la Commune d'accorder une attention plus forte à la sécurisation de ses installations industrielles.

4.1.3 Protection des données

Dans le cadre de ses activités, la Ville traite un nombre important de données personnelles. Celles-ci concernent notamment ses habitantes et habitants, clientes et clients, membres du personnel, entreprises, et divers partenaires. La Ville a depuis longtemps pris en compte cette réalité. Depuis l'adoption du règlement européen sur la protection des données personnelles en 2016, le traitement des données personnelles a connu des évolutions majeures, comme par exemple :

- le renforcement des droits des personnes concernées et de la responsabilisation des sous-traitants ;
- l'obligation de gérer la sécurité des données personnelles selon une approche par les risques et d'avertir les autorités compétentes (pour le Canton de Vaud : l'Autorité de protection des données et de droit à la transparence, (APDI)) et les personnes concernées en cas d'incident majeur ;
- le renforcement du régime de sanctions (notamment le montant des amendes pouvant être prononcées en cas de violation des exigences légales) et des pouvoirs des autorités compétentes (par exemple l'APDI) ;
- le renforcement des attentes des personnes concernées.

En 2017, face à ces évolutions, la Municipalité a décidé de renforcer sa capacité de mise en conformité avec les exigences légales. Elle a confié cette mission à la Commission à la protection des données personnelles[1], qui est chargée de traiter et de valider les mesures à prendre, avant soumission à la Municipalité. Enfin, la Municipalité a adopté en 2021 le document intitulé « Lignes directrices relatives à la protection des données personnelles ». Ce document formalise la stratégie que la Ville entend mettre en œuvre pour gérer les problématiques liées à la protection des données.

Les principes stratégiques de protection des données[2] doivent être concrétisés au travers d'une démarche de mise en conformité des traitements entreprise à l'échelle de la Ville. En effet, depuis l'annonce de la révision du droit suisse, tant sur le plan fédéral que cantonal, les autorités compétentes, en l'occurrence l'APDI pour les autorités communales du Canton de Vaud, ont considérablement renforcé leur niveau d'exigence et comptent multiplier les contrôles auprès des entités soumises à leur surveillance.

4.2 Bilan du précédent préavis N° 2015/73 « Renforcement de la sécurité des Systèmes d'information pour la période 2016-2019 »

Dans le cadre du précédent préavis, les améliorations envisagées couvraient les trois axes suivants :

1. renforcement des systèmes et des solutions informatiques ;
2. contrôles et gestion des accès ;
3. gouvernance de la sécurité de l'information.

Les paragraphes qui suivent précisent, pour chacun de ces axes, quelles mesures sont opérationnelles, quelles mesures sont encore en cours de déploiement.

Il est à noter que le précédent préavis ne couvrait pas les besoins liés à la protection des données.

---

[1] La Commission à la protection des données personnelles a pour membres la Directrice du Logement, de l'environnement et de l'architecture en charge de l'informatique, la cheffe du Service d'organisation et d'informatique, le responsable de la sécurité informatique et le premier conseiller juridique du Secrétariat municipal.

[2] Les définitions des cinq principes stratégiques de protection des données figurent dans l'annexe 3.

4.2.1 Renforcement des systèmes et des solutions informatiques

Depuis 2015, la Ville a renforcé le niveau de sécurité global de son SI via le déploiement des mesures techniques et organisationnelles suivantes :

- solutions de protection contre les codes malicieux et les virus de dernière génération ;
- centres de traitement des données (c'est-à-dire datacenters) hautement sécurisés ;
- réseaux informatiques segmentés et résilients face aux pannes ;
- infrastructure matérielle et logicielle de détection des vulnérabilités sur les composants techniques du SI ;
- dispositifs de déploiement régulier des correctifs de sécurité fournis par les éditeurs ;
- dispositifs de sauvegarde et de restauration des données traitées au sein du SI ;
- dispositifs de filtrage des e-mails indésirables.

Cependant, les mesures en place doivent être poursuivies, améliorées, complétées ou simplement renouvelées pour faire face aux nouvelles menaces, comme précisé au paragraphe 6.5.

4.2.2 Contrôles et gestion des accès.

Dans ce domaine, la Ville a principalement renforcé les processus et les dispositifs techniques d'authentification des utilisatrices et utilisateurs. La liste des mesures déployées comporte notamment :

- dispositifs d'authentification unique SSO[3] permettant d'accéder à de nombreuses applications de la Ville en ne procédant qu'à une seule authentification ;
- dispositifs d'authentification à double facteur, impliquant qu'une utilisatrice ou un utilisateur ne puisse accéder au SI de la Ville via VPN[4] qu'après avoir présenté deux preuves d'identité distinctes ;
- augmentation de capacité des dispositifs d'accès à distance dans le cadre des besoins de télétravail liés à la pandémie de COVID-19.

Les autres domaines liés à la gestion des identités et des accès (par exemple la gestion des arrivées et des départs, la gestion des droits dans les applications, etc.) sont toujours embryonnaires et constituent un axe d'amélioration prioritaire. Une partie conséquente du présent préavis consistera à préparer les infrastructures pour la mise en place de cette gestion.

4.2.3 Gouvernance de la sécurité de l'information

1. pour assurer la gouvernance de la sécurité du SI, la Ville de Lausanne a déployé un dispositif de gouvernance appelé SMSI[5]. Ce système organisationnel, basé sur une approche pragmatique d'amélioration continue, comporte cinq grands piliers :
2. un registre des risques de cybersécurité et un plan de traitement y relatif ;
3. une politique de sécurité de l'information, incluant les règles et les standards à respecter ;
4. des mécanismes de contrôle de la conformité et de l'efficacité des mesures de sécurité ;
5. une gestion de l'organisation « sécurité » de la Ville et des compétences humaines nécessaires ;
6. un référentiel documentaire géré avec rigueur et accessible à tout le personnel.

[3] SSO : Single Sign On en anglais, authentification unique en français.

[4] En anglais : Virtual Private Network (ou réseau privé virtuel).

[5] Système de management de la sécurité de l'information.

Bien que le SMSI soit aujourd'hui opérationnel, les mesures suivantes doivent être renforcées :

- la gouvernance des informations (classification, responsable, référentiels, etc.) ;
- la sensibilisation et la formation du personnel aux risques de sécurité de l'information ;
- l'amélioration et l'entraînement du plan de secours informatique et de gestion de crise.

5. Enjeux pour la Ville

La sécurité de l'information et la protection des données ne sont ni des produits, ni des états, mais des processus perpétuels. Leur mise en place exige une prise de conscience forte : le risque numérique doit faire partie intégrante des risques opérationnels gérés par la Ville et ne relève plus des seules équipes informatiques ou juridiques. La sécurité et la protection des données sont essentielles pour faire face aux enjeux majeurs auxquels la Ville est confrontée dans le monde du numérique. Les enjeux sont détaillés en annexe 4.

6. Réalisations envisagées dans le cadre du présent préavis

6.1 Gestion coordonnée des incidents de sécurité

Pour protéger son système d'information, la Ville met en œuvre une politique de sécurité visant en priorité à prévenir les incidents de sécurité. Cependant, bien que cette approche préventive permette de limiter le risque, il est techniquement et humainement impossible de le réduire totalement. Par conséquent, il est important que la Ville envisage à l'avance les scénarios d'incidents les plus vraisemblables auxquels elle pourrait être confrontée, et se prépare à réagir pour garantir une réponse rapide, efficace et adéquate.

Pour traiter correctement ce thème, la Ville doit aligner la gestion actuelle des incidents aux meilleures pratiques du domaine, cadrée par les référentiels et normes en vigueur, en mettant en œuvre les activités suivantes de manière systématique : la détection, le traitement et l'analyse des incidents ainsi que l'amélioration de la sécurité.

La mise en œuvre concrète comprend le renforcement des mesures suivantes, qui permettent de détecter tous les évènements qui se produisent :

- le dispositif technique de collecte des événements et de détection des incidents de sécurité ;
- le processus de tri et de première investigation ;
- les procédures d'analyse des évènements.

La gouvernance est cadrée par les procédures de gestion des incidents de sécurité, de violation de données et de gestion de crise, revues et documentées, qui feront l'objet d'une information et d'un exercice ad hoc auprès des acteurs identifiés pour chaque cas précis. Cependant, tout le personnel de la Ville doit être sensibilisé à la gestion des incidents, y compris de crises, afin d'adopter les bons réflexes et les bonnes pratiques.

6.2 Gestion des identités et des accès (GDIA)

La gestion des identités et des accès, qui comprend l'authentification des utilisatrices et des utilisateurs, l'attribution des autorisations et la supervision des accès sont un processus de sécurité essentiel. Une gestion des identités et des accès inefficace ou pire, inexistante, expose le SI à de nombreuses menaces.

La Ville doit construire une solution, organisationnelle et technique, permettant de gérer de manière simple le cycle de vie de toutes les usagères et tous les usagers, et de toutes les applications du SI. L'objectif global est de garantir que les bonnes personnes aient accès aux bonnes ressources, pour les bonnes raisons, au bon moment et dans les bonnes conditions. La mise en œuvre concrète de cette solution, qui impliquera obligatoirement des équipes métier, comprend entre autres le déploiement des mesures suivantes :

- une politique de gestion des utilisatrices et utilisateurs, de leurs droits et des comptes associés ;

- un dispositif, technique et organisationnel, de gestion du cycle de vie des utilisatrices et utilisateurs : arrivée (création des comptes et attribution des droits), changement (modification des droits) et départ (désactivation, puis suppression des comptes) ;
- un dispositif, technique et organisationnel, de gestion des comptes spéciaux (comptes d'administration et comptes techniques) ;
- un processus de surveillance des comptes et de leurs privilèges.

Mettre en place une gestion des identités et des accès (GDIA) est un vrai défi dans les institutions. Il s'agira de mettre en place les infrastructures techniques et la définition des prochaines étapes pour une intégration plus aisée d'une démarche globale de GDIA.

6.3 Sensibilisation et formation à la sécurité de l'information

Les utilisatrices et les utilisateurs sont devenus, pour les pirates, le vecteur privilégié de pénétration dans les SI. Il est en effet plus facile de duper une utilisatrice ou un utilisateur que d'essayer de contourner les systèmes de sécurité. Pour protéger son SI, la Ville a donc besoin de s'assurer que tout le personnel, indifféremment de son statut, de son rôle ou de sa mission, soit en mesure d'identifier les menaces, d'y faire face et d'adopter les réflexes sécuritaires adéquats.

Le programme de formation et de sensibilisation traitera les thèmes suivants :

- la sécurité de l'information (la protection des informations, quelles que soient leur forme) ;
- la cybersécurité (la protection du cyberespace constitué par le SI de la Ville) ;
- la responsabilisation du personnel dans l'exercice de sa fonction, avec diligence, conscience et fidélité, en s'abstenant de faire quoi que ce soit qui pourrait entraver la bonne marche du service, tout en prenant le plus grand soin du matériel mis à disposition et/ou utilisé.

La mise en œuvre concrète de ce programme, qui sera obligatoire pour toutes les collaboratrices et tous les collaborateurs et qui s'inscrira dans la durée en tant qu'activité permanente, comprend le déploiement des mesures suivantes :

- un dispositif d'inscription et d'évaluation en ligne des participantes et participants ;
- des sessions de sensibilisation standard pour 1000 collaboratrices et collaborateurs par an ;
- des sessions de formation spécifique selon les profils les plus exposés.

Le programme de formation et de sensibilisation a été préparé dans le cadre du préavis précédent. Son déploiement et son suivi se feront dans le cadre du présent préavis.

6.4 Contrôle de la conformité et de l'efficacité

L'erreur est humaine ! Ce constat factuel a une conséquence directe sur le niveau de sécurité du SI : tout système informatique peut, à un instant donné, ne pas être conforme aux règles de sécurité en vigueur, ou être en train de dériver imperceptiblement vers cette non-conformité. Afin de garantir la sécurité du SI en tout temps, il est fondamental de mettre en œuvre un processus visant à détecter les écarts le plus tôt possible, pour déclencher les corrections nécessaires.

Les actions envisagées dans ce préavis sont :

- la mise en œuvre d'un dispositif d'audit de sécurité ciblant prioritairement les éléments existants du SI les plus critiques ;
- la mise en œuvre d'un dispositif de validation de la robustesse de toutes les nouvelles solutions intégrées au sein du SI de la Ville face à de potentielles cyberattaques.

6.5 Renforcement des socles techniques

Bien que les dispositifs de sécurité techniques actuels (par exemple pare-feu, antivirus, accès à distance VPN, etc.) permettent de sécuriser les échanges de données entre le SI

de la Ville et l'extérieur, ces dispositifs doivent être améliorés, renforcés ou renouvelés pour garantir les niveaux d'exigence qu'impliquent la digitalisation des services, la réglementation sur la protection des données ou une migration partielle vers un Cloud suisse, selon les options envisagées dans la stratégie Cloud de la Ville.

La Commune devra mettre en œuvre un ensemble de solutions technologiques complémentaires visant à renforcer les socles techniques actuels. Ce renforcement couvrira notamment les thèmes suivants :

— la prévention des fuites de données ;

— la supervision des accès et usages Cloud pour la sensibilisation de tout le personnel, et le contrôle du type de données traitées ;

— le chiffrement et l'anonymisation des données sensibles.

6.6 Sécurité des systèmes d'information industriels

Un SI industriel est un système numérique, constitué d'un ensemble d'équipements et de logiciels, qui permet de surveiller et de contrôler un ou plusieurs procédés industriels (par exemple production d'électricité, transport d'eau potable, etc.). La généralisation de ces systèmes constitue pour les cyber-pirates une opportunité, et ce d'autant plus qu'il est difficile pour les exploitants d'en assurer la protection.

Sur ce thème, les points suivants seront traités dans le cadre du présent préavis :

— la mise en place d'une cellule interne de soutien « SI industriel » ayant pour mission de sensibiliser le personnel concerné aux cyber-risques et d'accompagner les services dans leurs démarches ;

— la poursuite des efforts de cloisonnement démarrés en accompagnant les équipes techniques à la migration de leurs équipements ;

— la conception et le déploiement de plateformes « poste de travail » et « serveur » dédiées et adaptées aux enjeux industriels ;

— la conception et la mise en œuvre, pour chaque installation industrielle, d'un plan de sauvegarde et de restauration approprié ;

— la mise en place d'un inventaire centralisé pour avoir une connaissance complète du parc d'équipements techniques (concentrateurs, automates, capteurs, etc.) ;

— l'exécution régulière de scans de vulnérabilités et la tenue d'un registre des vulnérabilités en collaboration avec les équipes techniques ;

— la définition de standards et la mise en œuvre d'un processus d'homologation afin de s'assurer de la prise en compte de la sécurité dès l'acquisition des équipements.

6.7 Protection des données

Afin de permettre à la Ville et aux différentes entités qui la composent de se conformer à la loi en matière de protection des données, il est nécessaire de définir et de mettre en œuvre une démarche globale permettant de gouverner et de gérer la manière dont les données personnelles sont traitées.

Le déploiement de cette démarche comprendra la mise en œuvre de cinq mesures :

— la mise en place et la tenue d'un registre qui recense, par direction et par service, les activités de traitement ;

— l'établissement d'une structure documentaire permettant d'instruire les exigences de la Ville ;

— la définition des règles de gestion des relations avec les sous-traitants qui traitent des données pour le compte de la Commune ;

— la définition et la mise en œuvre des contrôles appropriés permettant de vérifier la conformité ;

- la mise en place d'un programme de formation et de sensibilisation des collaboratrices et collaborateurs de la Ville intégré au plan de formation et sensibilisation à la sécurité du système d'information. Ce programme est obligatoire pour toutes les collaboratrices et tous les collaborateurs.

Le présent préavis permettra de financer les actions suivantes :

- la mise en place d'un outil d'inventaire et d'un outil d'analyse d'impact ;
- un renfort opérationnel pour effectuer les opérations prévues.

La démarche globale, validée par la commission à la protection des données, sera déployée en trois groupes de 12 services, dont les 12 premiers sont ceux qui traitent les données les plus sensibles.

7. Impact sur le climat et le développement durable

La mise en œuvre pratique d'une démarche d'informatique écoresponsable passe par plusieurs étapes, dont l'une concerne plus particulièrement ce préavis.

L'obsolescence des solutions et équipements informatiques constitue l'une des sources de vulnérabilités importantes pour le système d'information de la Ville. Les projets de sécurité soutiennent la lutte contre l'obsolescence et contribuent ainsi indirectement au développement durable.

8. Impact sur l'accessibilité des personnes en situation de handicap

Ce préavis n'a aucun impact sur l'accessibilité des personnes en situation de handicap.

9. Aspects financiers

9.1 Coûts prévisionnels

Type	Sous-type	Investissements *	Prestations **
6.1 Gestion des incidents	Dispositif de collecte	200'000	
	Processus de tri et d'investigation		80'000
6.2 GDIA (mise en place du socle)	Dispositif de gestion du cycle de vie	380'000	
	Dispositif de gestion des comptes		100'000
6.3 Sensibilisation	Mise en place	40'000	
	Coût de formation standard		160'000
	Coût de formation spécifique		100'000
6.4 Contrôle de la conformité	Dispositif d'audit des éléments critiques		420'000
	Dispositif de validation de la robustesse		100'000
6.5 Renforcement du socle technique	Dispositif de prévention fuite de données	80'000	
	Dispositif de supervision et contrôle des accès cloud	180'000	
	Dispositif de chiffrement et anonymisation des données	100'000	
6.6 Sécurité des systèmes d'information industriels	Conception et déploiement de plateformes		50'000
	Plan de sauvegarde		50'000
6.7 Protection des données	Outillage d'inventaire	40'000	
	Outil d'analyse d'impact	40'000	
	Renfort opérationnel		300'000
Totaux		**1'060'000**	**1'360'000**
		2'420'000	

*** Investissements :** acquisition de logiciels ou matériels ou dispositifs techniques permettant de remplir les fonctions citées dans ce tableau.
**** Prestations :** il s'agit de services fournis par des prestataires spécialisés dans les domaines cités (par exemple les audits sont réalisés par des auditeurs externes).

9.2 Incidences sur le budget d'investissement

Le crédit d'investissement se monte à CHF 2'420'000.- et figure au plan des investissements du Service d'organisation et d'informatique 2023-2026 au titre de «

Pilotage de la sécurité des systèmes d'information et de la protection des données ». Il prévoit la répartition des dépenses de la manière suivante :

(en milliers de CHF)	2023	2024	2025	2026	2027	2028	Total
Dépenses d'investissements	320	700	700	700			2420
Recettes d'investissements							0
Total net	**320**	**700**	**700**	**700**	**0**	**0**	**2420**

Dès lors, les moyens demandés seront affectés aux sept axes de travail décrits au chapitre 6 de ce document. Les appels d'offres restant à émettre, la répartition des financements des différents axes présentée sous le point 9.1 pourrait évoluer.

9.3 Incidences sur le budget de fonctionnement

	2023	2024	2025	2026	2027	2028	Total
Personnel suppl. (en EPT)							0
(en milliers de CHF)							
Charges de personnel							0
Charges d'exploitation		80	80	80	80	80	400
Charges d'intérêts		20	20	20	20	20	100
Amortissements		484	484	484	484	484	2420
Total charges suppl.	**0**	**584**	**584**	**584**	**584**	**584**	**2920**
Diminution de charges							0
Revenus							0
Total net	**0**	**584**	**584**	**584**	**584**	**584**	**2920**

9.3.1 Charges d'exploitation

Les droits d'utilisation logiciels et les maintenances annuelles associées aux investissements (hors prestations de service) ont un impact sur les charges d'exploitation du budget de fonctionnement. Cet impact est de CHF 80'000.- dès l'année 2024.

9.3.2 Charges d'amortissement

Le crédit d'investissement pour le pilotage de la sécurité des systèmes d'information et de la protection des données pour la période 2023-2026 se monte au total à CHF 2'420'000.-. Il est amorti sur cinq ans dès 2024 ; l'amortissement se monte à CHF 484'000.- par an.

9.3.3 Charges d'intérêts

Calculés sur la base d'un taux d'intérêt moyen de 1.5%, les intérêts théoriques moyens développés par le présent préavis s'élèvent à CHF 20'000.- à compter de l'année 2024.

10. Conclusions

Eu égard à ce qui précède, la Municipalité vous prie, Monsieur le Président, Mesdames, Messieurs, de bien vouloir prendre les résolutions suivantes :

Le Conseil communal de Lausanne,

vu le préavis N° 2023/47 de la Municipalité, du 28 septembre 2023 ;

ouï le rapport de la commission nommée pour examiner cette affaire ;

considérant que cet objet a été porté à l'ordre du jour,

décide :

1. d'adopter le programme de pilotage de la sécurité des systèmes d'information et de la protection des données pour la période 2023-2026 ;

2. de rendre obligatoires les formations identifiées pour la sécurité des systèmes d'information et pour la protection des données ;

3. d'allouer à cet effet à la Municipalité un crédit d'investissement du patrimoine administratif de CHF 2'420'000.- destiné à la gestion des projets, au développement ou à l'acquisition des solutions, ainsi qu'à leur adoption par les utilisatrices et utilisateurs ;

4. d'amortir annuellement la somme prévue sous chiffre 3 par le budget du Service d'organisation et d'informatique, rubrique n° 32.331 ;

5. de faire figurer sur rubrique n° 32.390 les intérêts relatifs aux dépenses découlant du crédit mentionné sous chiffre 3.

Au nom de la Municipalité

Le syndic
Grégoire Junod

Le secrétaire
Simon Affolter

Annexes :
1. Cas marquants d'attaques subies en Suisse et dans le monde
2. Liste des attaques subies par la Ville de Lausanne
3. Définition des principes stratégiques de protection des données
4. Enjeux pour la Ville

Annexes au préavis « Pilotage de la sécurité des systèmes d'information et de la protection des données pour la période 2023-2026 »

Annexe 1

Cas marquants d'attaques subies en Suisse et dans le monde

Le tableau ci-dessous liste quelques cas marquants de ces cinq dernières années en Suisse et dans monde.

Date	Cible et nature de l'attaque	Commentaires
10 octobre 2021	Administration communale de Montreux (VD, Suisse) : l'évaluation est encore en cours.	Evaluation en cours. *Plus d'information : 24heures.ch*
20 août 2021	Administration communale de Rolle (VD, Suisse) : vol des données personnelles de quelque 5000 habitants, données actuellement publiées sur le Darknet.	L'attaque était sophistiquée. S'y opposer nécessite des moyens techniques et humains appropriés, et une bonne organisation. *Plus d'information : RTS Info*
4 octobre 2020	Trois universités suisses, dont celle de Bâle : détournements de salaires, suite au vol de mots de passe par Phishing (hameçonnage).	Les criminels ont détourné un montant à six chiffres. Une partie des sommes se trouve désormais sur des comptes à l'étranger. *Plus d'information : RTS Info*
9 février 2021	Service des eaux de la Ville de Oldsmar (Floride, USA) : réseau d'eau potable contaminé par piratage informatique	Le piratage, découvert par hasard, utilisait un dispositif de prise de contrôle à distance mal configuré. *Plus d'information : swissinfo.ch*
10 mars 2021	Groupe aérien Swiss, via la société SITA, basée à Genève : vol des données personnelles des clients du programme de fidélité.	Attaque très sophistiquée. Vol important de données des clients de la société SITA, qui concernerait 1,35 million de passagers. *Plus d'information : Le Temps*
17 février 2021	Hôpitaux des villes de Dax et de Villefranche-sur-Saône (France) : sabotage des postes de travail par Ransomware, entraînant la paralysie des établissements.	L'ensemble des équipes ont opéré un retour forcé au papier et au stylo. Les blocs opératoires ont été mis en pause. *Plus d'information : Le Temps*
5 déc. 2020 **15 mai 2021**	Constructeur d'hélicoptères KOPTER (Wetzikon, Suisse) : vol de données suivi d'un sabotage des systèmes IT via un Ransomware, entraînant la paralysie du SI.	Kopter ayant refusé de payer la rançon, les données volées ont été diffusées sur le Darknet (dossiers commerciaux, contrats de défense, etc.) *Plus d'information : ZDnet.com, Le Temps*
14 mai 2021 **10 mai 2021**	Opérateur d'oléoducs Colonial Pipeline (USA) : sabotage des systèmes IT via un Ransomware, entraînant la paralysie de l'activité des principaux pipelines de la côte est des Etats-Unis.	Craignant une pénurie d'essence, Colonial Pipeline aurait accepté, avec l'accord du gouvernement, de verser une rançon de $ 5 millions aux pirates du groupe DarkSide. *Plus d'information : Le Temps, ICTJournal.ch*

Annexe 2

Liste des attaques subies par la Ville de Lausanne

Le tableau ci-dessous liste les attaques subies par la Ville ces cinq dernières années.

Période	Nature de l'attaque	Commentaires
12 septembre 2017	Infection de plus de 1'200 postes de travail par le logiciel malveillant EMOTET (cheval de Troie polymorphique difficile à détecter visant à collecter discrètement des données bancaires).	Une analyse poussée de tous les postes et serveurs de la Ville (environ 6'000) a dû être réalisée. Les coûts globaux de cette attaque sont estimés à plus de CHF 200'000.-.
28 juin 2021	Infection d'un poste de travail par un logiciel malveillant sophistiqué, piloté à distance sur Internet et se propageant sur d'autres postes.	L'intervention rapide des équipes a permis de contenir l'incident et de limiter ses effets.
Permanent	Attaques de phishing (hameçonnage) par vagues successives, visant à installer des logiciels malveillants (cheval de Troie, rançongiciel, etc.) sur les postes de travail.	Les techniques utilisées sont de plus en plus sophistiquées et permettent aux attaquants de franchir les barrières de sécurité de plus en plus fréquemment.

Annexe 3

Définitions des principes stratégiques de protection des données

1. Principe de responsabilité commune mais différenciée

Chaque collaboratrice ou collaborateur de la Ville ou chaque sous-traitant opérant pour le compte de la Ville doit être personnellement impliqué, en fonction de son rôle et de ses responsabilités, dans la mise en œuvre des exigences légales et/ou imposées par la Ville en matière de protection des données personnelles. Elle ou il doit, après avoir pris connaissance de ses droits et devoirs, reconnaître formellement ses responsabilités en la matière.

Au niveau de chaque direction ou service de la Ville, les autorités hiérarchiques sont responsables, sur leur périmètre de responsabilité, de l'application des exigences de la Ville en matière de protection des données personnelles. Ils doivent s'assurer que les consignes sont respectées et que les contrôles internes prévus par la Ville sont effectués.

2. Principe de gestion de la conformité

La gestion de la protection des données personnelles doit être basée sur un registre des activités de traitement régulièrement tenu à jour ainsi que sur l'établissement d'une stratégie pour identifier, analyser et traiter les non-conformités identifiées.

La gestion de la conformité se fait par l'adoption cohérente et concertée de mesures de prévention et de protection visant à éviter la violation des exigences applicables et en limiter l'impact en cas d'incident. Outre le degré d'impact pour les droits et libertés des personnes concernées, lesdites mesures tiennent compte du principe de cohérence, tel qu'exprimé ci-dessous, ainsi que de la nature, de la portée, du contexte et des finalités du traitement. Elles sont réexaminées et actualisées autant que nécessaire.

En outre, la mise en place d'une nouvelle activité de traitement ou la modification d'une activité de traitement existante doit faire l'objet d'une analyse permettant d'appréhender la licéité et les impacts potentiels sur les droits et libertés des personnes concernées.

3. Principe de cohérence

Toutes les exigences et pratiques relatives à la protection des données adoptées au sein de le Ville, sans égards à leur nature ou forme, doivent être, dès leur publication officielle :

- conformes à la législation applicable ;
- alignées avec la stratégie globale de la Ville ;
- cohérentes avec les moyens, humains et financiers, dont dispose la Ville, et applicables, immédiatement ou à court terme, dans le cadre de ces moyens.

Les sous-traitants œuvrant pour le compte de la Ville doivent se voir imposer contractuellement, ou par tout autre moyen contraignant, le respect des exigences en matière de protection des données personnelles applicables au sein de la Ville.

4. Principe de gestion du cycle de vie et d'amélioration continue

Les données personnelles sont protégées depuis leur collecte jusqu'à leur destruction ou anonymisation définitive. Par conséquent, les exigences et mesures adoptées par la Ville doivent couvrir toutes les étapes du cycle de vie des données personnelles.

En outre, toute solution ou service permettant le traitement de données personnelles doit prendre en compte, dès sa conception, les exigences applicables en la matière, qui ne doivent pas être traitées "à part" ou "après".

Le respect des exigences adoptées par la Ville doit être contrôlé de manière appropriée ; les principes et les moyens de contrôle interne adéquats doivent être inclus dès le départ et effectués sur une base régulière. Lors des contrôles, tout constat de non-conformité avec

une ou plusieurs exigences de protection des données, ou avec la législation en vigueur, ne doit pas être ignoré et doit faire l'objet d'un signalement à la hiérarchie, puis résolue par des mesures appropriées.

L'ensemble des processus permettant d'assurer la protection des données personnelles doit être audité régulièrement. Les éventuels dysfonctionnements observés ne doivent pas être ignorés, et seront pris en compte comme des opportunités de contribuer à la démarche globale d'amélioration continue de la protection des données personnelles.

5. Principe de transparence

Toutes les exigences applicables et toutes les décisions importantes prises dans le cadre de la gestion de la protection des données personnelles doivent être formalisées dans des documents. Cette documentation liée à la protection des données personnelles (politiques, directives, décisions, résultats d'audit, etc.) doit être gérée avec rigueur sur la base de processus clairement définis (élaboration, validation, enregistrement, classement, diffusion et mise à jour) et connus de tous les acteurs impliqués.

Les documents relatifs à la stratégie et à la politique de la Ville en matière de protection des données personnelles doivent être connus par tous les acteurs concernés (collaboratrices et collaborateurs de la Ville, sous-traitants, etc.). La dernière version en vigueur de chaque document doit être facilement accessible. Afin de faciliter la compréhension et l'approbation de la politique de la Ville en matière de protection des données, un programme de sensibilisation et de formation couvrant tous les besoins pédagogiques des acteurs concernés doit être défini et mis en œuvre.

La politique de contrôle et de supervision de la Ville en la matière doit être connue par tous les acteurs concernés ; les objectifs et modalités de mise en œuvre doivent être communiqués de façon totalement transparente.

Annexe 4

Enjeux pour la Ville

La sécurité de l'information et la protection des données ne sont ni des produits, ni des états, mais des processus perpétuels, des activités. Leur mise en place exige une prise de conscience forte : le risque numérique doit faire partie intégrante des risques opérationnels gérés par la Ville et ne relève plus des seules équipes informatiques ou juridiques. Les paragraphes suivants explicitent l'importance de la sécurité et de la protection des données pour le déploiement de politiques publiques essentielles.

1.1 Cyberadministration

La cyberadministration a pour objectif de permettre à la population et aux entreprises de traiter leurs affaires importantes avec les autorités par voie électronique, grâce aux technologies de l'information et de la communication. La stratégie suisse de cyberadministration[1] poursuit les trois objectifs suivants :

1. l'économie effectue les transactions administratives avec les autorités par voie électronique ;
2. les autorités modernisent leurs processus et communiquent entre elles par voie électronique ;
3. la population peut régler ses affaires importantes avec les autorités par voie électronique.

Pour que ces objectifs soient atteints, il est impératif que la protection des données et la sécurité de l'information soient prises en compte à un stade précoce et dans une mesure appropriée. Par ailleurs, dans un tel contexte, tout incident de sécurité peut avoir des conséquences importantes. Par conséquent, sans cybersécurité et sans protection des données personnelles, il ne peut y avoir de cyberadministration sûre et efficace.

1.2 Ville intelligente (smart city)

Une *smart city* a pour objectif d'offrir une qualité de vie élevée à ses habitants et à ses entreprises tout en consommant le minimum de ressources, grâce notamment à une connexion entre les systèmes d'information et de communication des bâtiments, des sites et des villes[2]. Pour être considérée comme une *smart city*, une ville doit être en mesure de répondre à différents critères définis par SuisseEnergie, notamment :

- exploiter de façon efficiente des formes d'énergie propres, ce qui implique une gestion numérique en temps réel des ressources ;
- gérer de façon optimale les transports publics et le trafic routier, ce qui implique une intégration poussée de l'informatique dans les moyens de transport et les infrastructures ;
- appliquer le principe de transparence en offrant à la population un accès ouvert aux données (notion d'*open data*), tout en garantissant la confidentialité des données sensibles et personnelles ;
- développer de nouveaux lieux et modes de travail, basés sur la collaboration, tout en réduisant les déplacements, ce qui implique le développement d'outils informatiques appropriés.

Dans tous ces domaines, une *smart city* utilise intensivement les technologies numériques. Cela implique que tous les systèmes informatiques qui supportent ces domaines soient sécurisés. En effet, un incident de sécurité peut affecter significativement le système d'information, allant possiblement jusqu'à la paralysie totale. Sans sécurité de l'information et

[1] Source : E-Governement Suisse (https://www.administration-numerique-suisse.ch/fr).

[2] Source : programme SuisseEnergie (https://www.suisseenergie.ch/)

sans protection des données personnelles, il ne peut y avoir de projet *smart city* réussi. Il s'agit de deux prérequis indispensables.

1.3 Souveraineté numérique

L'expression « souveraineté numérique » englobe une multitude de concepts, mais peut se résumer aux deux définitions suivantes :

- pour un individu, la souveraineté numérique est la maîtrise de son passé, son présent et de son futur tels qu'ils se manifestent et s'orientent par l'usage des nouvelles technologies de l'information ;
- pour une administration publique ou un état, elle désigne sa capacité à agir dans le cyberespace en préservant ses intérêts et ceux de ses usagères et usagers, à le réguler et peser sur l'économie numérique.

En l'espace de quelques années, l'Internet est devenu l'épine dorsale de nos sociétés, engendrant une dépendance aux nouvelles technologies et aux entreprises qui les contrôlent. Cette dépendance ne peut qu'augmenter avec le temps. Les faits survenus dans l'actualité récente (p.ex. cybersurveillance massive de citoyens, manipulation d'élections libres, opérations de déstabilisation à distance, espionnage économique, etc.) mettent en lumière les nouveaux défis auxquels sont confrontés les états, les acteurs économiques et la population elle-même. Bien qu'elles ne constituent pas une réponse unique à cet enjeu majeur, la sécurité de l'information et la protection des données sont des conditions nécessaires à la souveraineté numérique.

1.4 Évolution vers l'informatique en nuage (cloud computing)

Depuis plusieurs années, l'informatique connaît à l'échelle mondiale une évolution fondamentale et inexorable : les solutions historiquement hébergées dans les centres de données des entreprises (solutions sur site, *on-premise* en anglais) sont petit à petit externalisées, le plus souvent sur des infrastructures partagées accessibles via Internet. Ces solutions sont désignées par le terme informatique en nuage (*cloud computing* en anglais), et généralement par le terme Cloud.

Les moteurs de cette évolution sont multiples :

- le Cloud fournit des services qui répondent aux nouveaux modes de travail (nomadisme, télétravail, etc.) : applications en ligne, accessibles partout, à tout moment, etc. ;
- le Cloud fournit des services délivrés à la demande et facturés à l'usage, ce qui permet aux organisations de dégager des économies financières substantielles ;
- les grands éditeurs (p.ex. Microsoft, Oracle, SAP, etc.) investissent de moins en moins dans les solutions traditionnelles au profit des solutions Cloud. Certains ont même annoncé l'arrêt de la commercialisation de plusieurs de leurs produits phares *on-premise* ;
- le Cloud est d'ores et déjà omniprésent dans le quotidien des collaboratrices et collaborateurs, tant dans leur sphère privée que professionnelle, par exemple lors de l'usage de solutions telles que WhatsApp, Google Docs, Gmail, Facebook, Dropbox ou Swiss Transfer.

Le Cloud offre de réelles opportunités. Néanmoins, il présente également des risques, notamment juridiques, que la Ville doit gérer (par exemple le risque de ne pas pouvoir récupérer les données en cas de faillite ou de rachat, le risque de non-conformité du service avec la loi sur la protection des données, etc.). Plusieurs services différents offerts par le Cloud pourraient être envisagés, par exemple la location de certaines applications, l'utilisation de plateformes de développement, l'utilisation d'infrastructures, dont les choix seraient dépendants du niveau de sécurité et de la conformité à la protection des données.

Ainsi, sans sécurité de l'information et sans protection des données personnelles, il ne peut y avoir de mise en place de solutions Cloud. En clair, les données sensibles au sens de la loi resteraient à la Ville, les données non sensibles pourraient être mises sur un Cloud. Et pour finir, l'objectif est de travailler avec des Clouds locaux regroupant différents grands acteurs et/ou en tous cas des Clouds suisses.

1.5 Transformation numérique

Aujourd'hui, l'ensemble du personnel est amené à traiter en continu et le plus efficacement possible une quantité toujours plus grande d'informations, sous des formes variées et évolutives. Or, les usages en matière d'organisation, établis à l'ère du tout papier, n'ont pas été collectivement revus et repensés pour s'adapter à un environnement toujours plus numérique.

Cette nouvelle donne impose de restructurer les processus et les systèmes sous-jacents pour mieux accompagner les services dans la transition vers le tout numérique. Dans ce contexte, la mise en œuvre de la sécurité de l'information et de la protection des données personnelles, dès le début (« by design ») avec une approche zéro confiance (voir chap. 7.8), permettra de mettre en œuvre des pratiques et des solutions moins contraignantes et plus faciles à adopter.