

**Demande de crédit de CHF 95 500,00  
pour l'obtention du label Cyber-Safe**

Monsieur le Président,  
Mesdames les Conseillères communales,  
Messieurs les Conseillers communaux,

## 1. Objet du préavis

Le présent préavis a pour objectif de demander un crédit de CHF 95 500,00 TTC permettant de résoudre les différents problèmes relevés lors de l'analyse des cyber-risques et ainsi permettre de compléter la certification « Cyber-Safe » pour les services de l'administration communale.

## 2. Préambule

Dans le cadre du préavis 32/2023<sup>1</sup> dédié à la sécurité informatique, la Municipalité vous informait de sa volonté de réaliser un audit de sécurité informatique après application de mesures urgentes de sécurisation du réseau avec, comme objectif, d'obtenir une labellisation garantissant la sécurité informatique.

### Résultats de l'audit

L'audit a été réalisé à l'été 2024 et a fait l'objet d'une première version du rapport d'analyse, qui a été reçu le 30 juillet 2024, puis d'une version finale datée du 10 septembre 2024, mise à jour en particulier avec les résultats du test de phishing<sup>2</sup>.

Ce rapport évalue spécifiquement le coût que des incidents liés à la cybersécurité pourraient avoir sur les activités de l'administration communale à environ CHF 40 500,00, avec un niveau global d'exposition évalué comme moyennement critique et une attention particulière à porter sur la confidentialité des données, ce qui ne représente pas une surprise pour une administration communale.

Selon les informations collectées lors de l'audit, le niveau global de protection est jugé moyen (note de 5,8 sur 10), alors que le niveau de risque est mauvais (7,3 sur 10), en particulier au vu de la confidentialité des données gérées.

<sup>1</sup> Approuvé par votre Conseil le 14 septembre 2023

<sup>2</sup> Pour des raisons évidentes de sécurité, ce rapport ne peut être joint au présent préavis. Il sera cependant volontiers mis à disposition des membres des commissions nommées.

Enfin, le rapport mentionne 24 priorités à mettre en place pour améliorer ces scores :

- une mesure de très haute priorité (déjà résolue par notre fournisseur) ;
- huit mesures de haute priorité ;
- onze mesures de moyenne priorité ;
- deux mesures de basse priorité.

Sur ces 22 mesures, 21 d'entre elles sont requises pour obtenir la certification Cyber-Safe.

La mesure de très haute priorité est la conséquence de trois vulnérabilités de niveau critique détectées lors du scan du réseau. Deux d'entre elles venaient de l'ancienne GED (qui n'avait jamais été remise à jour par le prestataire GED depuis son installation) qui, depuis, a pu être retirée et supprimée, réglant ainsi le problème<sup>3</sup>. La dernière vulnérabilité est liée à des switchs (commutateurs) qui ne font pas partie de l'inventaire, situés dans les bâtiments de la voirie et au Rosset.

### **Actions nécessaires pour obtenir la certification**

Le présent préavis vise à couvrir les dépenses induites par les actions nécessaires permettant de régulariser ces mesures. Ces actions, globalement présentées, sont les suivantes :

#### Mise en place d'une politique de sécurité des systèmes d'information (PSSI)

Cette action primordiale vise à créer, rédiger et faire valider une PSSI qui va refléter la vision stratégique de la Municipalité. Elle doit permettre de poser un cadre définissant les objectifs à atteindre et les moyens nécessaires. Une fois établie, elle sera diffusée aux employés, ainsi qu'aux sous-traitants.

Les thèmes suivants devront, au moins, être abordés dans ce document :

- Procédure de gestion des utilisateurs (arrivée, changement de poste, départ).
- Règles et procédures de définition des accès informatiques (serveur de fichiers et logiciels).
- Règles et procédures de gestion du matériel et des logiciels.
- Règles et procédures liées à la sauvegarde et la restauration des données.
- Règles et procédures liées à la protection des données.
- Règles et procédures liées à l'élimination des supports de données.
- Règles et procédures liées à la cyber-résilience en cas d'attaque du réseau.
- Procédure de traitement des alertes de sécurité.
- Procédure de rotation des clés de sécurité (clés VPN, Wifi, etc.).
- Règles d'accès à la salle des serveurs.

L'ensemble des actions suivantes doit permettre soit de compléter, soit de valider les différents points énoncés ci-dessus.

---

<sup>3</sup> Voir à ce propos le préavis 20/2022 sur la mise à jour des archives et de la GED.

### Réaliser un inventaire complet de l'infrastructure et des données

Nous devons pouvoir disposer d'un inventaire exhaustif et à jour du matériel informatique connecté sur notre réseau, ainsi que des données qui y figurent ; chacune de ces données doit faire l'objet d'une politique de fréquence de sauvegarde, de conservation et de règles d'accès.

Afin de pouvoir, dans un deuxième temps, appliquer les règles définies par la PSSI, il conviendra de réaliser tout d'abord un inventaire initial décrivant de la situation actuelle.

### Faire valider nos sous-traitants

L'administration communale ne disposant pas d'un département informatique, les tâches liées aux systèmes d'information sont en quasi-totalité confiées à des entreprises externes.

Afin d'assurer notre propre sécurité, nous devons nous assurer que l'ensemble des sous-traitants mettent également en œuvre leurs propres mesures, via un label, une certification ou un engagement contractuel au moins équivalent aux exigences Cyber-Safe.

### Tester la restauration des données

Dans le cadre du préavis 20/2022, nous avons mis en place une politique de sauvegarde des données. Si des essais de restauration de documents à petite échelle ont été menés pour s'assurer du bon fonctionnement de ces outils, il s'agit maintenant de vérifier « grandeur nature » l'efficacité de la procédure de restauration des données.

Cette tâche va entraîner un coût supplémentaire d'environ CHF 1 000,00 lié au transfert de données depuis le système de sauvegarde (Microsoft Azure) sur les serveurs restaurés.

### Établir et faire signer une charte d'utilisation

Chaque collaborateur et utilisateur doit signer un document définissant ses droits et devoirs vis-à-vis des ressources informatiques. Cette charte doit également définir les droits et devoirs spécifiques des utilisateurs utilisant des équipements privés pour accéder aux ressources informatiques communales (principalement les membres de la Municipalité).

Ce document doit enfin préciser l'utilisation prévue des téléphones portables privés, du courrier électronique professionnel et de l'internet dans le cadre du travail.

### Déployer un gestionnaire de mots de passe

L'une des règles de base de la sécurité informatique réside dans la protection des mots de passe contre les accès non autorisés ; ils ne doivent en aucun cas être stockés sur un support (électronique ou physique) sans être chiffrés.

La solution recommandée dans ce cas consiste dans la mise en place d'un outil de gestion des mots de passe qui sera géré et déployé de manière centralisée sur l'ensemble des postes de travail.

Bien entendu, une telle solution est payante et devrait augmenter le budget informatique annuel d'environ CHF 80,00 par utilisateur, soit environ CHF 2 400,00 par an.

### Création d'un plan de reprise des activités

Dans le cas d'une défaillance de tout ou partie de l'infrastructure informatique, il s'agit de disposer d'un document clair, exhaustif et à jour, permettant de limiter les impacts en garantissant la continuité des activités ou une reprise la plus rapide possible de celles-ci.

Ce plan de reprise d'activité doit permettre d'assurer la reconstitution de l'infrastructure informatique dans différents modes d'exécution (mode dégradé, mode minimum, mode fonctionnel).

### Renforcement de la sécurité sur l'infrastructure réseau et serveur

Afin de renforcer encore davantage la sécurité, il est crucial de procéder à la mise à jour des switchs mentionnés plus haut, d'installer des certificats de sécurité et de procéder à la migration du serveur de messagerie vers Microsoft Office 365.

En effet, la mise en place de la double authentification requise pour la labélisation sur Exchange 2016 ne permet pas de couvrir l'ensemble des flux réseaux. De plus, la version d'Exchange 2016 arrivant en fin de vie, il sera nécessaire d'effectuer une migration dans les prochaines années

De surcroît, le chiffrement systématique sur les périphériques mobiles professionnels doit être mis en œuvre pour protéger les données sensibles en cas de perte ou de vol des appareils.

### Résumé des actions et évaluation du temps et des moyens nécessaires

#	Mesure	Heures de travail			Autres coûts CHF
		Rédaction	Technique	Validation	
1	PSSI	50	8	5	-
2	Établir la liste des permissions d'accès	10	42 <sup>4</sup>	2	-
3	Établir l'inventaire du matériel et des logiciels	7	16	2	-
4	Établir la liste des données	20	8	5	-
5	Faire valider nos sous-traitants	20	-	5	-
6	Tester la sauvegarde des données	5	4	1	500,00 <sup>5</sup>
7	Établir une charte d'utilisation	8	-	2	-
8	Gestionnaire de mots de passe	5	16	1	2 400,00
9	Renforcement de la sécurité	-	60	5	-
10	Plan de reprise des activités	30	16	1	-
11	Migration de la messagerie	-	64	8	12 000,00
12	Remplacement switchs réseaux	-	16		3 500,00
<b>Total</b>		<b>155</b>	<b>236</b>	<b>24</b>	<b>18 400,00</b>

<sup>4</sup> 28 heures pour le technicien informatique et 14 heures pour l'archiviste afin de mettre à jour le plan de classement.

<sup>5</sup> Ce montant représente le coût de transfert des données depuis Microsoft Azure.

La commune ne possédant ni service informatique, ni ressources disposant du temps et des compétences nécessaires pour réaliser ces différentes actions, il sera indispensable d'engager temporairement des ressources externes, à savoir :

- Pour la rédaction des différents documents, un analyste informatique disposant d'une spécialisation en cybersécurité et d'une connaissance du fonctionnement des communes vaudoises. Le coût d'un tel profil est évalué à environ CHF 150,00 / heure HT.
- Pour les aspects techniques, un technicien en informatique disposant des accès et de la connaissance du fonctionnement de notre système d'information. Pour des raisons pratiques facilement compréhensibles, ces tâches devront être réalisées par notre fournisseur informatique qui facture ses interventions au prix de CHF 180,00 / heure HT.
- Enfin, les parties de gestion du projet, de validation et de coordination seront assurées par le secrétaire municipal.

### 3. Aspects financiers

#### Coûts du préavis

Les coûts de ce projet se divisent comme suit :

Rubrique	Élément	Qté	PU	Total
<b>100</b>	<b>Heures de travail</b>			<b>65 730,00</b>
101	Heures de travail (rédaction)	155	150,00	23 250,00
102	Heures de travail (technique)	236	180,00	42 480,00
<b>200</b>	<b>Divers</b>			<b>18 400,00</b>
201	Autres coûts	1	18 400,00	18 400,00
	<b>Total brut</b>			<b>84 130,00</b>
	Divers et imprévus (5 %)			4 206,50
	<b>Total HT</b>			<b>88 336,50</b>
	TVA 8,1 %			7 155,25
	<b>Total net arrondi</b>			<b>95 500,00</b>

#### Amortissement

Depuis le 1<sup>er</sup> janvier 2024, les durées d'amortissement des investissements sont fixées par la loi.

En l'occurrence, les logiciels et le matériel informatique sont amortis sur cinq ans dès l'aboutissement des travaux financés par le crédit, soit un montant annuel estimé à CHF 19 100,00.

## Financement

Cette dépense n'est pas incluse dans les « projets futurs - crédits à voter » du budget 2025.

La Municipalité propose le financement de ce projet par prélèvement sur la trésorerie courante ou, au besoin, sur les lignes de crédits disponibles, dans la limite du plafond d'endettement.

## Coûts récurrents

Outre le montant de l'amortissement défini plus haut, le seul coût récurrent concerne le logiciel de gestion des mots de passe avec un montant estimé à CHF 80,00 par an et par utilisateur.

Il faut toutefois noter que le label Cyber-Safe a une durée de validité de 2 ans, au terme desquels le processus de labélisation doit être renouvelé ; dès 2027, le montant correspondant (soit environ CHF 4 000,00) sera porté au budget de fonctionnement.

Avec un utilisateur supplémentaire tous les deux ans, l'impact planifié de ce préavis sur les budgets informatiques futurs sera donc le suivant :

	<b>2026</b>	<b>2027</b>	<b>2028</b>	<b>2029</b>	<b>2030</b>	<b>2031</b>
Amortissement	19 100,00	19 100,00	19 100,00	19 100,00	19 100,00	0,00
Logiciel	2 400,00	2 400,00	2 480,00	2 480,00	2 560,00	2 560,00
Labélisation	0,00	4 000,00	0,00	4 000,00	0,00	4 000,00
<b>Total</b>	<b>21 500,00</b>	<b>25 500,00</b>	<b>21 580,00</b>	<b>25 580,00</b>	<b>21 660,00</b>	<b>6 560,00</b>

## 4. Planification provisoire

La planification provisoire du projet est la suivante :

<b>Étape</b>	<b>Période</b>
Collecte des informations	mars 2025
Rédaction	d'avril à juin 2025
Migration de la messagerie	mai 2025
Remplacement des switchs réseaux	mai 2025
Certification	juin 2025

## 5. Conclusions

Au vu de ce qui précède, la Municipalité vous demande, Monsieur le Président, Mesdames les Conseillères communales, Messieurs les Conseillers communaux, de bien vouloir prendre les décisions suivantes :

### LE CONSEIL COMMUNAL DE ROMANEL-SUR-LAUSANNE

- vu le préavis municipal N° 69/2025 adopté en séance de Municipalité du 20 janvier 2025 ;
- ouï le rapport des commissions consultées ;
- considérant que cet objet a été porté à l'ordre du jour ;

#### DÉCIDE :

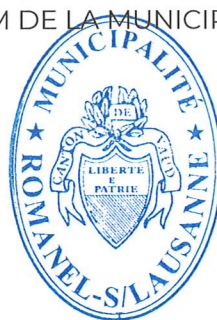
1. d'accepter le préavis municipal N° 69/2025 tel que présenté ;
2. d'accorder un crédit de CHF 95 500,00 pour la réalisation des travaux nécessaires devant amener à la labélisation Cyber-Safe ;
3. d'autoriser le financement de cette dépense par la trésorerie courante ou, au besoin, sur les lignes de crédit disponibles, dans les limites du plafond d'endettement.

AU NOM DE LA MUNICIPALITÉ

La Syndique :



Claudia Perrin



Le Secrétaire :



Nicolas Ray

Romanel-sur-Lausanne, le 20 janvier 2025

Délégué municipal : M. Denis Favre, Municipal

