



*MARCHE A PROCEDURE ADAPTEE  
DE TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION*

**ACCORD-CADRE DE PRESTATIONS DE SERVICES**

**SUIVI, MAINTIEN EN CONDITIONS OPERATIONNELLES  
ET EVOLUTIONS DE L'INFRASTRUCTURE INFORMATIQUE  
DE LA VILLE DE BISCHHEIM**

**CAHIER DES CLAUSES TECHNIQUES PARTICULIERES**

**Renseignements à solliciter par l'intermédiaire du site :**

**<https://www.alsacemarchespublics.eu>**

## Table des matières

1.	Cadre général .....	3
1.1.	Contexte .....	3
1.2.	Vocabulaire.....	3
1.3.	Prestations attendues .....	3
1.4.	Compétences attendues.....	3
2.	Questionnaire technique.....	4
3.	Descriptif de l'existant.....	5
3.1.	Plate-forme existante.....	5
3.2.	Contraintes à prendre en compte .....	8
4.	Prestations de suivi et de maintien en conditions opérationnelles.....	10
4.1.	Prise en compte de l'existant .....	11
4.2.	Vérifications régulières de l'infrastructure informatique .....	11
4.3.	Alertes de sécurité.....	11
5.	Prestations d'évolution de l'infrastructure .....	11
5.1.	Ajout de 2 To sur notre serveur PRA Dell T640.....	11
5.2.	Remplacement des switches / commutateurs du cœur de réseau .....	12
5.3.	Couverture Wifi d'un bâtiment .....	12
5.4.	Windows Server / Migration d'un serveur 2012 vers 2022 .....	12
5.5.	Projets spécifiques.....	13
5.6.	Familles matériels et logiciels.....	14

# 1. Cadre général

## 1.1. Contexte

Le service informatique de la ville de Bischheim exploite une plate-forme informatique située dans ses propres locaux, en complément de services hébergés par des tiers sur des plates-formes cloud.

L'objectif de cette consultation est de trouver un prestataire capable d'assurer le maintien en conditions opérationnelles de cette plate-forme, à la fois par des mesures préventives ou curatives, et de la faire évoluer selon les besoins de la ville.

La plate-forme en question s'entend au sens des éléments suivants : baie de stockage, serveurs physiques, switches, firewall et routeurs, machines virtuelles, sauvegardes, maintenance du serveur de secours, wifi et assistance ponctuelle (réseau) au prestataire en charge de la téléphonie IP.

## 1.2. Vocabulaire

- VM : virtual machine, machine virtuelle, représentant les serveurs Windows ou Linux utilisés par la ville, gérés par notre Vcenter.
- PRA : plan de reprise d'activité, et ici plus spécifiquement, le serveur de secours PRA stockant des répliques inactives des VM principales.

## 1.3. Prestations attendues

- Interventions régulières et préventives pour vérifier le bon état de l'infrastructure, assurer les mises à jour logicielles ou firmware des éléments de l'infrastructure.
- Vérification régulière de la bonne marche des backups, essais préventifs de restauration afin de vérifier que la lecture des backups est bonne.
- Suivi des patches de sécurité des logiciels clés de l'infrastructure
- Suivi des contrats de maintenance et de mise à jour des équipements : alerte en amont des fins de contrat pour lancer les renouvellements
- Sur des projets précis : mise en œuvre des évolutions demandées
- Conseil sur l'architecture et l'évolution de l'infrastructure
- Toutes les interventions doivent se faire dans le respect des normes de sécurité informatiques telles qu'elles sont recommandées par les constructeurs, les éditeurs des solutions en place et par l'ANSSI de façon générale.

## 1.4. Compétences attendues

Nous attendons aussi du prestataire qu'il maintienne à un haut niveau de compétence de ses équipes intervenant sur ce dossier, par rapport aux produits et technologies utilisées.

Le prestataire qui répond à cette consultation devra fournir le CV des intervenants en précisant le niveau de leurs compétences et la durée de leur expérience professionnelle respective dans les domaines suivants :

- Architecture système et réseau, VPN, VLAN
- Système d'exploitation Windows Server : administration système et réseau
- Système d'exploitation Linux : ne fait pas partie de cette consultation, en dehors de la gestion des sauvegardes des VM Linux.
- Matériel : Switchs manageables notamment de modèle CISCO SG350X / SG 300 ou C9200L
- Firewalls de marque : Fortinet (Fortigate).
- Gestion de Machines Virtuelles VMWare VCenter
- Système de sauvegarde Veeam

- Téléphonie IP de type Alcatel : ne fait pas partie de cette consultation, en dehors de la gestion des accès réseau et VLAN requis par la téléphonie IP
- Matériel : Serveurs Physiques Dell ESX
- Baie de stockage Dell PowerStore
- Logiciel antivirus Cisco Secure Endpoint
- Compétences générales en terme de cyber-sécurité, afin que toutes les interventions respectent les règles et l'état de l'art en matière de cyber-sécurité.

## 2. Questionnaire technique

**Dans son mémoire technique, le prestataire fournira impérativement des réponses** aux questions suivantes, qui représentent un test de compétence concret dans les différentes technologies en place à la ville :

- FIREWALL > Comment voir la liste des personnes qui sont connectées en VPN à notre infrastructure ? (produit utilisé pour la connexion VPN : Fortigate 101F)
- FIREWALL > Comment couper en urgence tous les accès VPN à notre site principal ? (produit utilisé pour la connexion VPN : Fortigate 101F)
- VPN > Aucun agent en télétravail n'arrive à se connecter au VPN géré par les FortiGate. L'erreur affichée est « Unable to establish the VPN connection. The VPN server may be unreachable ». Quelle est votre démarche de diagnostic pour trouver le problème ?
- INTEGRATION TELEPHONIE IP A L'INFRA > Sur un switch CISCO, quelles sont les étapes pour paramétrer un VLAN spécifique pour la téléphonie IP d'un port donné ?
- VEEAM > Une sauvegarde Veeam d'une VM bloque avec l'erreur suivante : « [Backup job failed. Cannot create a shadow copy of the volumes containing writers data. VSS asynchronous operation is not completed. Operation: [Shadow copies commit] ». Quelle est votre démarche de diagnostic et de résolution du problème ?
- VM ET PARTITIONS WINDOWS > Sur un serveur Windows virtualisé, il y a 2 disques C et D. Le disque C est presque plein. Toutefois l'augmentation classique de la taille de C ne fonctionne pas sur le Vcenter car C et D sont sur le même volume. Comment faire pour augmenter malgré tout la taille de C ?
- CISCO SECURE ENDPOINT > Nous souhaitons qu'un site internet précis soit interdit d'accès depuis tous nos PC équipés de Cisco Secure Endpoint. Pouvez-vous décrire la démarche pour paramétrer cela ? (notons que nous ne souhaitons pas utiliser une règle de nos Fortigate pour cette question, car plusieurs PC passent par une connexion privée ou depuis des bâtiments non équipés de Fortigate)

## 3. Descriptif de l'existant

### 3.1. Plate-forme existante

#### 3.1.1. Architecture globale

Les services informatiques fournis par la ville de Bischheim à ses usagers sont partiellement hébergés par la ville, et partiellement hébergés par des prestataires extérieurs. Ce cahier des charges ne concerne que les services hébergés par la ville de Bischheim dans ses locaux.

Les serveurs sont hébergés dans un local technique principal situé à l'hôtel de ville. Un serveur de secours utilisé dans le cadre d'un Plan de Reprise d'Activité (PRA) est localisé dans un autre bâtiment de la ville. Les sauvegardes sont transférées sur un autre site également. En complément de ces sauvegardes en ligne, des sauvegardes hors ligne, sur bandes, sont également stockées dans un autre lieu que l'hôtel de ville.

Le local technique principal et le site du PRA sont reliés par une fibre optique propriétaire. Chacun de ces deux sites dispose de sa propre connexion Internet par fibre optique, celle du PRA servant de secours à celle du site principal en cas de coupure.

#### 3.1.2. Services fournis aux usagers

Les services fournis par les infrastructures informatiques de la ville sont les suivants :

- Annuaire (Active Directory)
- DNS (Microsoft)
- Messagerie et agenda (Microsoft Exchange 2019 au jour de publication de ce document)
- Partage de fichiers (Windows network share)
- Serveur d'impression (Microsoft)
- Partage de fichiers spécifiques à certains utilisateurs à gros volume (Windows network share sur NAS)
- Cloud de partage de document (owncloud sur Linux)
- Applications web PHP/mysql spécifiques (archives, état civil sur Linux)
- Logiciel RH (Berger Levraut / Base Oracle fournie par l'éditeur)
- Logiciel finances (Berger Levraut / Base Oracle fournie par l'éditeur)
- Logiciel état civil (Base Oracle fournie par l'éditeur / client serveur)
- Bureau à distance pour usagers de l'état civil
- Accès VPN à distance pour les usagers en télétravail ou sur d'autres sites
- Backup quotidien des VM sur le même site (voir plus loin pour les backups déportés)
- Filtrage d'accès et sécurité générale des flux (firewall Fortinet)
- Wifi Pro : wifi public pour le guichet unique de l'hôtel de ville et les salles de réunion. Possibilité pour chaque agent de s'authentifier sur le Wifi des agents. Serveur Utopia pour les authentification Wifi.
- VM Alcatel pour la téléphonie IP (fait l'objet d'un marché différent, cité ici pour information)
- Serveur Windows de gestion des certificats

#### 3.1.3. Sites

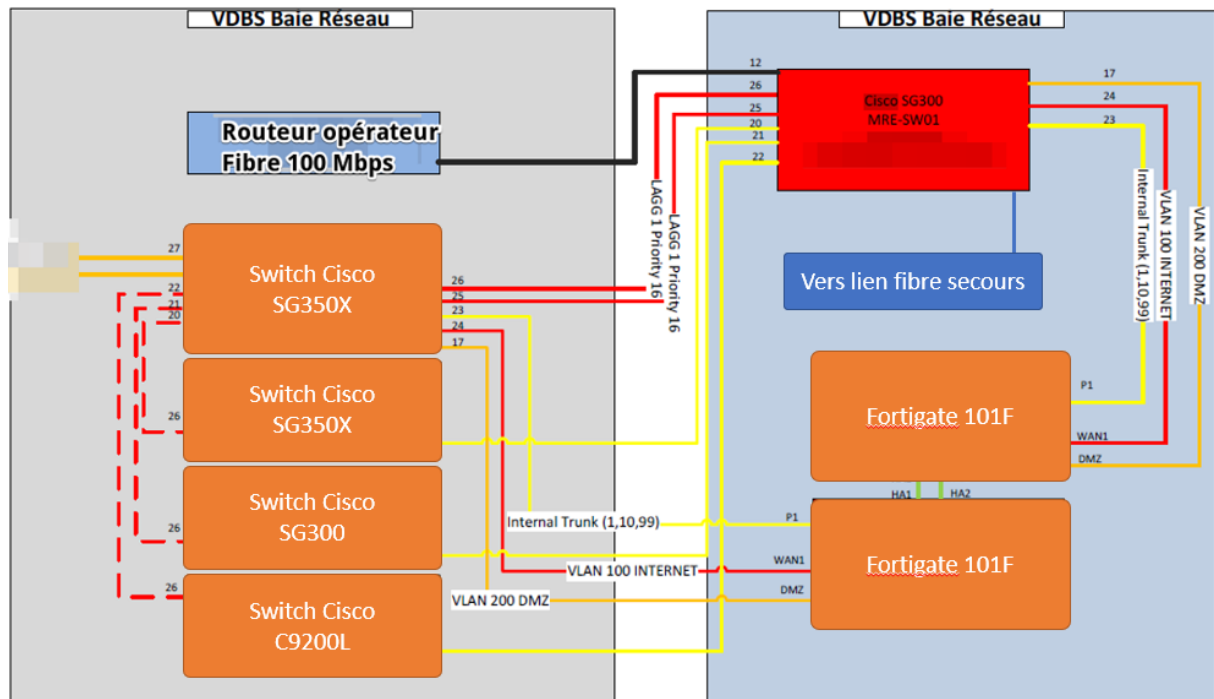
##### 3.1.3.1. Site principal

Le local technique principal est situé à l'hôtel de ville. Il est composé de :

- 2 serveurs physiques Dell ESX R650 XS abritant toutes les VM utilisées, Windows et Linux
- 1 baie de stockage Dell PowerStore 500T reliée aux serveurs physiques

- 1 serveur de gestion des backups Dell T440 disposant de son propre stockage et d'un lecteur de bandes
- 2 pare-feux Fortinet 101F redondants en High Availability (HA)
- 1 équipement télécom Alcatel pour la téléphonie IP (fait l'objet d'un marché différent, cité ici pour information) connecté à un routeur de téléphonie SFR.
- Des switches Cisco pour le cœur de réseau SG350X
- Des switches Cisco pour les PC utilisateurs SG300 ou 9200L
- Un onduleur électrique Eaton
- Des équipements de l'opérateur télécom (SFR/Comptel) pour la connexion Fibre : RAD, routeur SFR.
- Des équipements de l'opérateur télécom (Orange) dédiés à certains postes de l'Etat Civil et gérés en direct par l'ANTS, Agence Nationale des Titres Sécurisés. Ce réseau est totalement indépendant de la connexion Internet de la ville et ne dessert que 2 PC spécifiques qui ne sont connectés qu'à l'ANTS.
- Une clim, un déshumidificateur et un contrôle d'accès double, par badge électronique et par clé physique

Schéma du cœur de l'infrastructure :



### 3.1.3.2. Machines virtuelles (VM) en service

Avec OS Windows Server

- Mercury : gestion des badges d'accès / serveur historique peu utilisé
- Mre-affdyn : gestion affichage dynamique des écrans
- Mre-fs01 : fichiers partagés, serveur d'impression
- Mre-pc-virtual1 : pc client pour tests
- Mre-ucopia : gestion des accès wifi
- Mre-vcenter : gestion des VM
- Saturne2 : applications métier des services ressources, base Oracle installée par l'éditeur

- Mre-dc01 : active directory
- Mre-exch19-01 : Microsoft Exchange 2019
- Pluton : serveur pour les accès bureau à distance permettant d'utiliser les applications état civil (clients lourds)
- Mre-dc02 : VM hébergée par le serveur de PRA et faisant office d'AD de secours synchronisé avec Mre-dc01.

Avec OS Linux, gérant des applications web diverses (souvent en PHP/mysql)

- Mre-supervision-01 : serveur Zabbix supervisant tout le réseau et l'infrastructure
- Neptune
- Srvweb
- Terra
- Tux-02

### 3.1.3.3. Sites annexes

Un site appelé ABC est relié à l'hôtel de ville par une fibre optique dédiée, et dispose d'une connexion fibre séparée qui sert de secours au site central.

D'autres sites annexes : Sapin Vert, Villa, Bibliothèque, Salle du Cheval Blanc sont reliés à Internet de façon autonome, mais connectés au site central en VPN via des équipements Fortinet. Certains de ces sites disposent de la téléphonie IP comme le site central et le Sapin Vert

### 3.1.4. Sauvegarde et PRA

Un serveur de sauvegardes quotidiennes est situé dans le local technique principal. Il effectue de façon hebdomadaire une sauvegarde sur bandes hors ligne, stockée dans un lieu séparé.

Par ailleurs, la ville dispose d'un site annexe relié en fibre optique privée au local technique principal. Il est équipé de :

- 1 serveur de PRA Dell disposant de son propre stockage
- 2 NAS de marque QNAP utilisés pour stocker des répliqués des backups réalisés dans le local technique principale
- 1 serveur Proxy utilisé pour accéder aux QNAP en iSCSI

### 3.1.5. Postes de travail

En comptant l'hôtel de ville et le site ABC, une centaine de postes de travail fonctionnent sur le réseau.

### 3.1.6. Télétravail et accès distant (usagers et administration)

De nombreux agents accèdent aux services à distance, soit depuis leur domicile en télétravail, soit depuis un site distant qui n'est pas connecté directement au réseau de la ville.

Les modalités d'accès retenues sont : établissement d'un VPN via Forticlient, établissant la liaison entre le PC de l'utilisateur et le réseau de la ville. La gestion du VPN est réalisée sur le Fortinet central de la ville, connecté à l'annuaire AD. Le compte de l'agent doit faire partie d'un groupe spécial de l'AD autorisé à se connecter au réseau de la ville.

Le service informatique ainsi que le prestataire pourront également accéder aux serveurs via ce même moyen, afin d'intervenir à distance sur la plate-forme.

## 3.2. Contraintes à prendre en compte

### 3.2.1. Délai des indisponibilités selon les services fournis

Les services sont utilisés aux heures de bureau : du lundi au vendredi de 8h-12h30 et 13h30-17h30. La mairie accueille du public en continu entre 8h et 17h sans coupure à midi. Toutefois de nombreux agents consultent la messagerie, accèdent aux logiciels métier ou au partage de document en dehors de ces horaires.

Les mises à jour de firmware, de logiciels ou plus généralement toute intervention entraînant l'indisponibilité d'un service devra être :

- Prévue en dehors des heures de bureau, sauf exception
- Planifiée à l'avance en lien avec le service informatique, afin de prévenir les usagers de la coupure de service
- 

### 3.2.2. Backups

Toute intervention sur l'infrastructure doit prendre en compte les backups en place, de sorte que ces backups ne soient pas impactés et/ou soient mis à jour.

Les backups en place :

- Quotidiens : chaque VM est backupée sur notre serveur de sauvegarde en salle machine, toutes les nuits
- Bi-hebdomadaires : chaque VM en exploitation est backupée sur le serveur de PRA 2x par semaine
- Hebdomadaire : backup des fichiers Veeam de chaque VM sur un QNAP
- Hebdomadaire : backup sur bandes des VM pour un stockage hors ligne

Par exemple, le changement d'IP d'un NAS nécessite la modification de la tâche de backup correspondante. L'ajout d'un serveur nécessite de l'intégrer dans le schéma de backup, donc d'installer le client du logiciel de backup et d'en faire le paramétrage.

En cas de modification ou de mise à jour des scripts de backup, il sera nécessaire de vérifier dans les jours qui suivent que les backups fonctionnent correctement.

### 3.2.3. Sécurité

Toute intervention sur l'infrastructure informatique doit être faite dans le respect des règles de sécurité informatiques, notamment en regard des recommandations préconisées par l'ANSSI ([Agence nationale de la sécurité des systèmes d'information \(ssi.gouv.fr\)](https://ssi.gouv.fr))

### 3.2.4. PRA (Plan de Reprise d'Activité) en cas de sinistre

À tout moment, l'ensemble des serveurs hébergés par la ville doit pouvoir être remonté sur le serveur de PRA, dans un délai inférieur à 48h (si possible 24h) à compter du moment où la ville demande au prestataire d'activer le PRA. L'adressage des serveurs, des machines, le routage général devra être mis en place pour pouvoir accéder à ses serveurs, à minima du bâtiment où se situe le PRA et si possible depuis l'hôtel de ville, qui dispose d'une fibre privée vers le bâtiment du PRA.

La mise en œuvre du PRA dépend de l'incident concernant le site central, il faudra pouvoir faire face à différents scénarios possibles, par exemple l'interconnexion rapide d'un nouveau site où les agents seraient replacés, si l'hôtel de ville n'est plus en mesure d'accueillir un système informatique.

Dans sa réponse technique, **le prestataire détaillera son plan précis de mise en route du PRA** dans le cas où la salle machine de l'hôtel de ville est totalement inexploitable.



### 3.2.5.RGPD

Le prestataire s'engage à respecter totalement la réglementation RGPD, en interne et dans le cadre de ses interventions pour le compte de la ville de Bischheim. S'il emploie des sous-traitants, il s'engage à vérifier qu'ils respectent également la réglementation RGPD.

Dans sa réponse, le prestataire indiquera qui est le Délégué à la Protection des Données (DPO) RGPD de sa structure.

### 3.2.6.Sobriété numérique

La sobriété numérique est « une démarche qui vise à réduire l'impact environnemental du numérique en limitant ses usages. Cela consiste à concevoir des services numériques plus sobres et à modérer ses usages numériques quotidiens » (source : Wikipedia).

Dans le cadre de sa réponse, le prestataire pourra suggérer des actions visant à améliorer la sobriété numérique de la plate-forme de Bischheim. Il indiquera également quelles sont ses compétences ou références dans le domaine.

### 3.2.7.Mise à jour de la documentation

Après chaque intervention ou chaque modification de la plate-forme, le prestataire fournira une mise à jour de la documentation technique de l'infrastructurem odifiée.

### 3.2.8.GTI et GTR et pénalités

Dans le cadre de la prestation de suivi et maintien en conditions opérationnelles, le prestataire devra tout mettre en œuvre pour respecter des délais d'intervention et de rétablissement, selon la gravité de l'incident. La ville pourra appliquer des pénalités financières si le prestataire ne respecte pas ces délais.

#### 3.2.8.1. Définitions

GTI, garantie de temps d'intervention : délai maximum pour que le prestataire mette à disposition de la ville une ou plusieurs personnes compétentes dans la résolution du problème soumis.

GTR, garantie de temps de rétablissement : délai maximum pour que le prestataire résolve le problème soumis. Le non respect de ces durées contractuelles peut donner lieu à des pénalités financières.

Ces valeurs dépendent de la classification des incidents, définie comme suit :

Type d'incident	Définition	Exemples
<b>Désastre (mise en œuvre du PRA)</b>	Tout incident très grave impactant la salle machine principale de l'hôtel de ville, ou le bâtiment, et empêchant le rétablissement en moins de 2 jours des services aux usagers.	Dégât des eaux détruisant les serveurs ; incendie ; vol
<b>Critique</b>	Tout incident empêchant globalement l'accès aux services, sans que la plupart des équipements actifs ne soient endommagés ou irréparables	Dysfonctionnement des switches cœur de réseau ; du firewall central ; de la baie de disque, de VMWare. Panne matérielle ou logicielle de l'un de ces équipements.

<b>Majeur</b>	Incident empêchant l'accès à un service majeur proposé aux usagers ; ou empêchant la bonne marche des sauvegardes	Incident bloquant l'AD, le partage de fichiers, les accès à distance en VPN, etc.
<b>Mineur</b>	Incident ne bloquant pas ou peu les usagers, incident contournable par une solution provisoire	Problème d'accès depuis un poste ; avertissement ou problème concernant une sauvegarde

Selon la gravité de l'incident, voici les délais maximums d'intervention en termes de GTI et GTR. Les heures ouvrées ou calendaires sont définies sous le tableau.

Type d'incident	GTI (heures ouvrées*)	GTR
<b>Désastre (mise en œuvre du PRA)</b>	2h ouvrées*	48h calendaires** pour la remontée du PRA et la mise en place des premiers accès aux serveurs, au moins depuis les postes situés dans le bâtiment du PRA.
<b>Critique</b>	4h ouvrées*	8h ouvrées* (sauf si l'incident concerne la connexion Internet fournie par l'opérateur télécom de la ville, ou un élément hors de la responsabilité du prestataire)
<b>Majeur</b>	6h ouvrées*	48h calendaires**
<b>Mineur</b>	3 jours ouvrés*	15 jours calendaires***

\* Heure/jour ouvrés : lundi au vendredi de 8h-12h30 et 13h30-17h30, jours fériés exclus

\*\* Heure calendaire : 24H/24, 7j/7

\*\*\* Jour calendaire : chaque jour de la semaine, samedi et dimanche inclus

Pénalités en cas de dépassement de la GTI ou GTR :

Type d'incident	GTI	GTR
<b>Désastre (mise en œuvre du PRA)</b>	200 € par heure ouvrée* de retard	200 € par heure calendaire** de retard
<b>Critique</b>	100 € par heure ouvrée* de retard	50 € par heure ouvrée* de retard
<b>Majeur</b>	50 € par heure ouvrée* de retard	25 € par heure ouvrée* de retard
<b>Mineur</b>	50 € par jour calendaire*** de retard	10 € par jour calendaire*** de retard

Les modalités d'application des pénalités sont explicitées dans le CCAP.

#### 4. Prestations de suivi et de maintien en conditions opérationnelles

Ces prestations se feront sur la base de bons de commande faisant référence au bordereau de prix.

#### 4.1. Prise en compte de l'existant

Le prestataire dispose d'un délai maximum de 20 jours calendaire pour prendre en compte l'ensemble de l'infrastructure réseau existante, à compter de la notification du marché. Il chiffrera dans son mémoire technique le nombre de jours et le type de profils mobilisés de son côté pour cette démarche ; il détaillera le plan précis de ses interventions pour prendre en compte l'existant. Enfin il chiffrera le temps sollicité auprès du service informatique de la ville pour l'aider à prendre en compte cet existant.

#### 4.2. Vérifications régulières de l'infrastructure informatique

Le prestataire indiquera à quelle fréquence et pour quelle durée il mobilisera ses équipes pour réaliser une vérification de l'infrastructure, à titre préventif.

L'objectif de ces contrôles est de vérifier la bonne marche de l'ensemble de l'infrastructure, et de réaliser des mises à jour de firmware ou de logiciels recommandées par les éditeurs, constructeurs ou par le prestataire, de vérifier que les sauvegardes sont bien effectuées. Par « infrastructure », nous entendons :

- L'infrastructure de sauvegarde (serveur de backup, veeam et son paramétrage, backup sur le PRA et les cartouches)
- Les firewalls du site central
- Les switches Cisco cœur de réseau
- La baie de stockage PowerStore
- Les serveurs physiques ESX gérant les VM
- La gestion des VM et les mises à jours du Vcenter
- L'Active Directory
- L'antivirus Cisco Secure Endpoint
- Le serveur Exchange 2019

C'est dans le cadre de cette prestation de maintien en conditions opérationnelles que le prestataire s'engage à intervenir en cas d'incident, selon les GTI et GTR détaillées précédemment dans ce document. S'il reste un solde de journées d'intervention dans ce que le prestataire a prévu dans la prestation de maintien en conditions opérationnelles, le temps d'intervention pour résoudre l'incident en sera décompté. Dans le cas où il ne reste plus de jours, la ville commandera les jours manquants sur la base du tarif des journées d'intervention, prévu au bordereau de prix.

#### 4.3. Alertes de sécurité

Le prestataire sera pro-actif et signalera au service informatique toute mise à jour de sécurité urgente qui pourrait concerner l'un de ses équipements. Il détaillera de quelle structure de veille de sécurité il dispose et de combien d'experts en sécurité sont actifs sur cette tâche.

### 5. Prestations d'évolution de l'infrastructure

Ces prestations se feront sur la base de bons de commandes faisant référence au bordereau de prix. Voici le détail de ces prestations attendues :

#### 5.1. Ajout de 2 To sur notre serveur PRA Dell T640

##### 5.1.1. Cible souhaitée

- Nous souhaitons disposer de 2 To utiles sur notre PRA, qui dispose actuellement de 12 disques physiques de 480 Go. Actuellement notre PRA est presque plein, il reste environ 360 Go sur 4,8 To utiles.

- Cette prestation doit être clef en main : achat des disques, installation sur site et configuration du PRA pour qu'il prenne en compte le nouveau gain de place.

#### *5.1.2. Modalités d'intervention et de coupure des services*

Le PRA pourra être coupé en journée le temps nécessaire pour l'intervention. La seule VM en production est le DC02 qui peut être coupé de façon planifiée. Le prestataire indiquera toutefois quel est le temps de coupure estimé pour cette intervention.

### **5.2. Remplacement des switches / commutateurs du cœur de réseau**

#### *5.2.1. Cible souhaitée*

Cette prestation consiste en la mise en place de nouveaux switches de cœur de réseau, en remplacement des switches actuels, connectant les serveurs physiques de VM, les firewalls, les switches « utilisateurs », les deux routeurs opérateur pour la connexion Internet (principale et de secours). Configuration minimale souhaitée ces 2 switches :

- 24 ports, 4x10G Uplink
- Alimentation principale et secondaire
- Les switches doivent être redondants autant que possible
- Maintenance matérielle et logicielle souhaitée : garantie classique
- 

#### *5.2.2. Modalités d'intervention et de coupure des services*

Le prestataire détaillera son plan d'intervention pour le remplacement des switches actuels, notamment sa méthodologie de récupération des configurations actuelles, de leur reprise sur les nouveaux switches. Il donnera une idée du temps de coupure pour les utilisateurs.

### **5.3. Couverture Wifi d'un bâtiment**

En partant du principe qu'un bâtiment ou qu'une école dispose d'une connexion Internet filaire, cette prestation consiste à poser des bornes Wifi pro et un contrôleur de bornes Wifi, afin d'assurer la couverture Wifi du bâtiment.

Un réseau wifi « grand public » sera disponible, et séparé d'un réseau wifi « agents ». Dans le cas d'un Wifi pour une école, le prestataire détaillera les solutions proposées pour réaliser un filtrage d'accès Internet pour le réseau wifi « grand public » (qui sera le réseau pédagogique), et pour le wifi « agents » conforme aux recommandations de l'éducation nationale.

Le bordereau de prix prévoit des lignes différentes en fonction du nombre de bornes à poser, qui dépend de l'étendue du bâtiment.

La prestation doit inclure la pose et la configuration des bornes Wifi, étant entendu que des prises RJ45 POE seront fournies au prestataire aux endroits où les bornes devront être posées.

En cas de travaux électriques requis, la ville prendra en charge ces travaux qui ne seront pas à la charge du prestataire.

### **5.4. Windows Server / Migration d'un serveur 2012 vers 2022**

#### *5.4.1. Cible souhaitée*

Cette prestation consiste à migrer en Windows Server 2022 (ou version la plus à jour au moment de la commande) un serveur qui est en version Windows 2012 R2.

Il s'agit du serveur MRE-FS01 qui sert essentiellement à partager des fichiers auprès de nos utilisateurs connectés via un partage de type `\\MRE-FS01\mairie`. Ces partages font l'objet de droits d'accès selon des groupes de sécurité, gérés dans l'AD, et qui doivent être repris à l'identique sur le nouveau serveur. Ce serveur propose aussi une dizaine d'imprimantes réseau partagées, et gérées par des GPO sur l'AD. Le nouveau serveur devra reprendre ce partage des imprimantes.

#### *5.4.2. Modalités d'intervention et de coupure des services*

Le prestataire détaillera son plan d'intervention pour cette migration, en veillant à minimiser l'interruption de service, et à mettre en œuvre un support réactif dans les jours qui suivent la migration.

Il expliquera s'il privilégie la conservation de la même IP et nom Windows pour le nouveau serveur lors de la bascule, ou s'il préfère que le serveur ait une autre IP et un autre nom, ce qui nécessitera une nouvelle GPO de mise en place des PC et sans doute des interventions sur les PC qui auraient par exemple des raccourcis avec l'ancien nom.

### **5.5. Projets spécifiques**

#### *5.5.1. Ajout de 20, 30 ou 40 CAL Exchange 2019*

Nous disposons actuellement de 270 Cals Exchange 2019. Cette prestation consiste à en acheter un lot de 20, 30 ou 40 licences supplémentaires, et à les intégrer dans notre serveur Exchange 2019.

#### *5.5.2. Test complet de remise en route du PRA*

L'objectif de ce test est de s'assurer que le PRA est totalement autonome des équipements de la salle machine principale, et que le remontage des VM se fait dans de bonnes conditions et dans un temps maîtrisé.

Afin de ne pas interférer sur les serveurs et le réseau réel, un réseau totalement séparé physiquement sera monté à l'occasion de ce test : switch + PC client connectés au PRA, sans connexion Internet.

Le prestataire détaillera les opérations et les tâches qu'il mettra en œuvre pour réaliser ce test, et le temps nécessaire pour faire l'ensemble du test.

#### *5.5.1. Test complet de bon fonctionnement des sauvegardes réalisées avec Veeam*

L'objectif de ce test est de s'assurer que les sauvegardes de VM réalisées quotidiennement avec Veeam sont bien fonctionnelles et peuvent être récupérées. Le prestataire expliquera sa démarche.

#### *5.5.2. Déplacement du PRA sur un nouveau site physique*

Prestation consistant à déplacer le PRA et ses équipements associés (switch, QNAP de sauvegarde externe, PC proxy réalisant le montage disque du QNAP de sauvegarde) sur un autre site. La prestation doit comprendre le réadressage réseau et le reparamétrage de la sauvegarde sur le PRA.

#### *5.5.3. Installation d'une nouvelle VM dans l'architecture (intégrant la sauvegarde, le PRA, les exports QNAP, les licences)*

La ville pourra demander à créer une nouvelle VM dans l'infrastructure et demander au prestataire de l'intégrer dans l'infrastructure globale, ce qui inclut :

- La sauvegarde Veeam : intégration de la nouvelle VM dans la sauvegarde quotidienne ; dans la sauvegarde hebdomadaire sur les QNAP, dans la sauvegarde vers le PRA et sur les cartouches de sauvegarde. Vérification des dimensionnement disque. Test et vérification de la sauvegarde sur les premières itérations de sauvegarde
- L'achat des licences logicielles si nécessaire selon l'OS de la nouvelle VM (ligne du BPU séparée pour cet achat de licence)

## **5.6. Familles matériels et logiciels**

Le bordereau de prix demande au prestataire le coût d'une année de garantie et d'une année de maintenance et de support logiciel, pour l'ensemble des composants de l'infrastructure de la ville. Merci de vous reporter au bordereau de prix pour la liste des éléments demandés.

Ce bordereau demande aussi le prix unitaire de l'ajout (ou du remplacement) d'un composant de l'infrastructure, comme l'ajout d'un disque de 1,9 To sur la baie de stockage, l'ajout d'un switch cœur de réseau aux caractéristiques comparables à celles détaillées précédemment dans le document.

Fait à Bischheim, le 12 septembre 2024

Signé

Le Maire

Jean-Louis HOERLE