

# **CAHIER DES CLAUSES TECHNIQUES PARTICULIERES (CCTP)**

**Services d'infogérance pour le CTLes**

Marché n° 2025-3

## Table des matières

<b>1</b>	<b>Contexte général</b>	<b>4</b>
1.1	Présentation du CTLes	4
1.2	Objet du marché	4
1.3	Objectifs du marché	5
<b>2</b>	<b>Présentation de l'existant</b>	<b>6</b>
2.1	Organisation	6
2.2	Infrastructures IT	6
2.2.1	Inventaire des actifs	6
2.2.2	Infrastructures et Architectures	8
2.2.3	Infrastructures techniques	10
2.3	Applications et services	10
2.3.1	Applications métiers	10
2.3.2	Logiciels	11
2.4	Autres	11
2.4.1	Nom de domaine	11
2.5	Infogérance actuelle : services et statistiques	11
2.5.1	Services actuels d'infogérance	11
2.5.2	Statistiques des demandes et des incidents	12
<b>3</b>	<b>Prestations attendues</b>	<b>12</b>
3.1	Prestations à l'initialisation du marché	12
3.2	Prestations initiales	14
3.2.1	Sauvegarde	14
3.2.2	Sécurisation des flux internet et accès à distance	14
3.3	Les prestations de base	15
3.3.1	Gestion du parc informatique	15
3.3.2	Gestion des applications	16
3.3.3	Gestion de nom de domaine	17
3.3.4	Sécurité du SI	17
3.3.5	Sauvegarde et restauration	19
3.3.6	Monitoring (surveillance opérationnelle et de sécurité) du parc	20
3.3.7	Gestion des incidents et des demandes	21
3.4	Prestations complémentaires	24
3.4.1	Demande de prestations	24
3.4.2	Anti-malware	25
3.4.3	Création et déploiement d'un master	25
3.4.4	Evolution majeure du master	25
3.4.5	Installation d'un nouveau poste de travail	26
3.4.6	Evolution de l'infrastructure locale	26
3.5	Documentation	26
3.6	Organisation de la prestation	27
3.6.1	Interlocuteurs de référence	27
3.6.2	Comitologie : phase mise en œuvre initiale	27
3.6.3	Comitologie : phase d'exploitation	27

3.7	Mise en œuvre .....	28
3.7.1	Architecture .....	28
3.7.2	Méthodologie et organisation .....	28
3.7.3	Planning de mise en œuvre .....	28
3.8	Vérification d'aptitude (VA), Vérification de service régulier (VSR) .....	29
3.8.1	Vérification d'Aptitude (VA) .....	29
3.8.2	Vérification de Service Régulier (VSR) .....	29
3.9	Limites de la prestation .....	30
3.10	Réversibilité et transférabilité .....	30
<b>4</b>	<b>Développement durable / RSE .....</b>	<b>31</b>
4.1	Développement durable .....	31
4.2	Responsabilité sociétale .....	31
<b>Annexe 1</b>	<b><u>Présentation des services assurés par l'uge.....</u></b>	<b><u>32</u></b>

CDRT Les indications dans les encadrés bleus ont pour but de faciliter le remplissage du cadre de réponse pour les soumissionnaires. Ils ne font pas parti du CCTP.

# 1 Contexte général

## 1.1 Présentation du CTLes

Le CTLes, créé en 1994, est un établissement public administratif sous la tutelle du Ministère de l'Enseignement Supérieur et de la Recherche situé à Bussy Saint-Georges (Seine et Marne).

La mission première du CTLes est d'offrir une bibliothèque de dépôt.

Le Centre Technique du Livre de l'enseignement supérieur (CTLes) est un établissement public administratif qui propose aux bibliothèques de l'enseignement supérieur d'Île-de-France un service de stockage à distance et de communication pour des collections à faible taux de rotation.

Le CTLes a également un rôle central dans le dispositif de gestion coopérative de la conservation des collections de périodiques imprimés à travers son support aux plans thématiques de conservation partagée des périodiques (PCP).

**Le CTLes** comprend une trentaine d'agents qui disposent pour la plupart de deux postes de travail, l'un dans les locaux du CTLes à Bussy Saint-Georges, l'autre au domicile de l'agent.

Le CTLes soustraite, via une convention de service, à l'Université Gustave Eiffel (UGE) toutes les activités d'infogérance de son système d'information. Cette convention prendra fin autour de la fin de l'année 2025

## 1.2 Objet du marché

Le CTLes lance une consultation en vue de retenir une Société d'infogérance qui prendra le relais de l'UGE. Ce prestataire assurera la reprise en main des infrastructures, services et prestations, dans le cadre de la mission d'infogérance qui lui est confiée

La prestation d'infogérance pour le CTLes, attendue à partir du 1<sup>er</sup> janvier 2026, comprendra les services suivants :

- La gestion, la maintenance, l'administration, le monitoring, le support utilisateurs et l'administration des :
  - o Environnements de poste de travail (matériel, OS)
  - o Des serveur(s) et système(s) associé(s)
  - o Des équipements réseaux (filaire et sans-fil)
  - o Et des équipements de sécurité
- Le maintien en conditions opérationnelles (MCO) et de Sécurité (MCS)
  - o Postes de travail et PC
  - o Des serveur(s) et système(s) associé(s)
  - o Des équipements réseaux (filaire et sans-fil)
  - o Et des équipements de sécurité

- La gestion des sauvegardes et des restaurations associées aux infrastructures incluses dans le périmètre.
- Des prestations de conseil portant sur la gestion de dossiers techniques, l'évolution, l'optimisation et la sécurisation des infrastructures ; le cas échéant des prestations de fourniture, installation, configuration et mise en œuvre

### **1.3 Objectifs du marché**

Les principaux objectifs visés par le présent marché sont :

- Le maintien du Système d'Information en conditions opérationnelles ;
- La garantie de la sécurité des actifs et des données ;
- Le conseil et la maîtrise d'œuvre sur toute évolution logicielle, matérielle ou d'infrastructure rendue nécessaire par l'activité du CTLes ou des contraintes extérieures ;
- Le conseil en matière de maîtrise et de visibilité des coûts relatifs au système d'information ;
- Le suivi de l'activité par l'intermédiaire d'indicateurs pertinents ;
- La réversibilité des services à tout moment.

## 2 Présentation de l'existant

### 2.1 Organisation

Le CTLes ne dispose pas d'une Direction des Systèmes d'Information (DSI).

La gouvernance du SI est gérée par :

- La direction du CTLes pour les aspects stratégiques
- La chargée du SI documentaire pour les aspects opérationnels. Le niveau de compétence est évalué à intermédiaire

### 2.2 Infrastructures IT

#### 2.2.1 Inventaire des actifs

Les équipements sont acquis par le CTLes.

##### Terminaux et périphériques<sup>1</sup>

Cat.	Type	Nb	Commentaire
Terminal	PC fixe	37	
Terminal	PC portable	27	
Terminal	Imprimante monoposte	9	Dont 2 en fin de vie
Terminal	Imprimante multifonction monoposte	1	
Terminal	Scanner monoposte	1	
Terminal	Copieur multi-fonction	2	Hors périmètre de la prestation d'infogérance objet du présent CCTP. Acquisition et maintenance via UGAP
Terminal	Scanner	1	Hors périmètre de la prestation d'infogérance objet du présent CCTP. Connexion au réseau uniquement.
Terminal	Haut-parleurs	3	
Terminal	Webcam	12	
Terminal	Matériel de visioconférence	1	Logitech group (utilisation de la caméra uniquement)
Terminal	Matériel d'audioconférence	2	Poly Sync 60
Terminal	Onduleur	1	En fin de vie
Terminal	Smartphone	2	Hors périmètre de la prestation d'infogérance objet du présent CCTP. Acquisition et maintenance gérées par le CTLes

Nota : Les collaborateurs qui effectuent du télétravail disposent de deux terminaux :

- 1 PC fixe situé à leur poste de travail dans les locaux du CTLes
- 1 PC portable utilisé à leur domicile

<sup>1</sup> Les références des actifs sont indiquées dans le fichier *DCE – Annexe 2 du CCTP.xlsx*

## Equipements d'infrastructure<sup>2</sup>

Cat.	Type	Nb	Commentaire
Infra	Serveur	1	En fin de vie Maintenance constructeur jusqu'en juillet 2026
Infra	Switch administrable	5	HP COMMUTATEUR Aruba 2530-48G 48*10/100/1000+4SFP
Infra	Switch non administrable	4	Divers
Infra	Bornes WIFI	2	Point d'accès WiFi Ubiquiti UniFi AP-AC-Pro
Infra	Bornes WIFI	5	Point d'accès WiFi Ubiquiti UniFi U6-PRO
Infra	Contrôleur WIFI	1	
Infra	Routeur CTLes	1	Appliance "maison" basée sur Linux

## Système de téléphonie d'entreprise

Le système de téléphonie et l'infrastructure associée (IPBX Mitel, switches PoE, ...) appartiennent à la Bibliothèque Nationale de France (BNF) qui partage le site de Bussy-Saint-Georges avec le CTLes et sont administrés par elle.

Le système de téléphonie est hors périmètre de la prestation d'infogérance, objet du présent CCTP.

## Licences

Le CTLes dispose d'un parc homogène en Windows 10.

Les licences sont de type OEM. Cependant lors de la masterisation des postes de travail, les licences sont remplacées par des licences de l'université.

Des actions sont en cours pour « récupérer » une preuve de possession des licences OEM.

Le CTLes est éligible aux lots 1 et 2 du marché d'acquisition de licences Windows de la centrale d'achat **Groupe Logiciel**, du Ministère de l'Enseignement Supérieur et de la Recherche, dont le titulaire est la société Crayon. Les lots 1 et 2 couvrent respectivement les licences EES, MPSA, CSP et les licences SPLA.

La garantie et la maintenance des logiciels sont assurées par les éditeurs au travers d'un marché via la centrale d'achat **Groupe Logiciel**.

---

<sup>2</sup> Les références des actifs sont indiquées dans le fichier *DCE – Annexe 2 du CCTP.xlsx*

## 2.2.2 Infrastructures et Architectures

### 2.2.2.1 Schéma d'architecture de principe

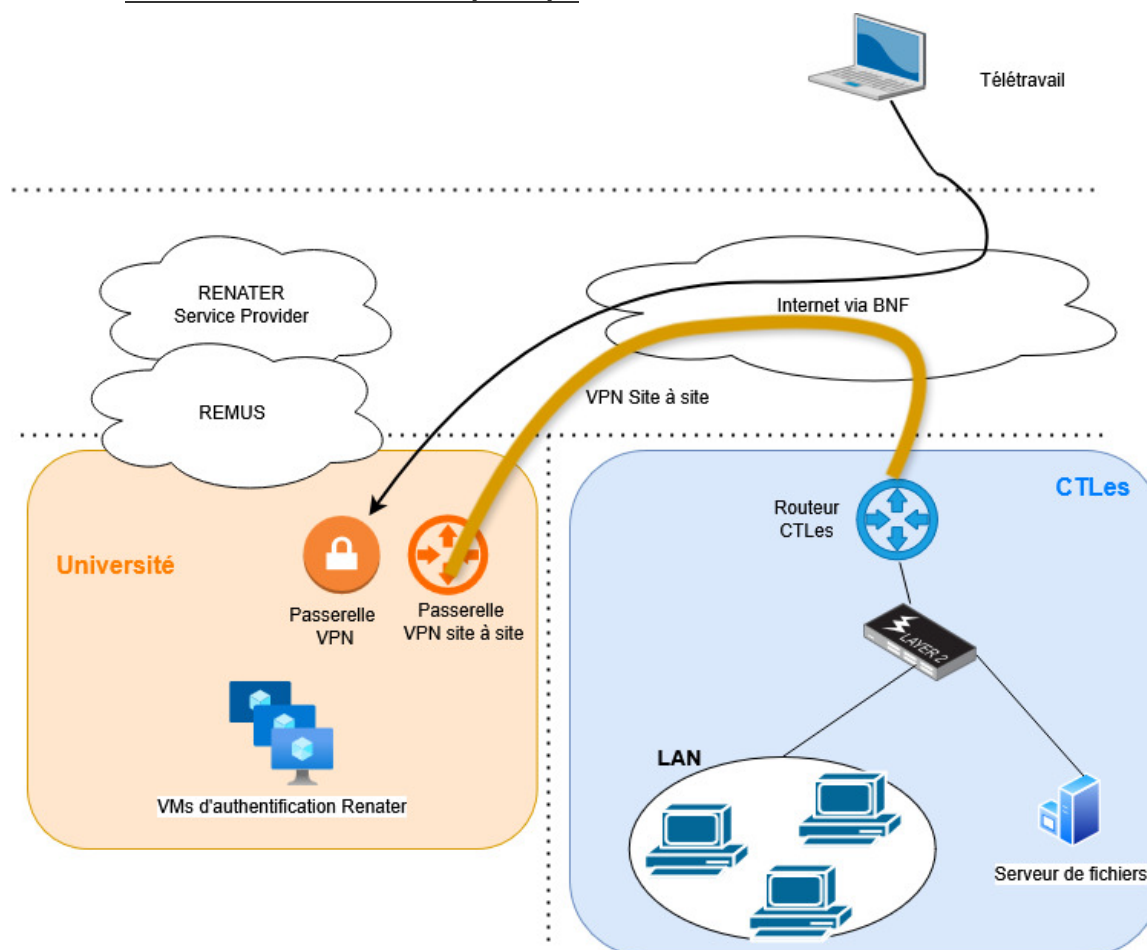


Figure 1 : Existant – Architecture de principe

Renater est le Réseau national de télécommunications pour la technologie, l'enseignement et la recherche reliant les établissements d'enseignement supérieur et de recherche publique (universités, centres de recherche, etc.).

### 2.2.2.2 Infrastructures LAN et WLAN

Le réseau se compose de switches administrables non PoE du constructeur HPE. Les switches sont installés dans les locaux techniques du siège du CTLes à Bussy Saint-Georges.

Des vlans sont configurés notamment pour :

- Les postes de travail
- Les « réseaux » wifi

L'infrastructure WLAN (WiFi) repose sur des équipements du constructeur UNIFY :

- Un Contrôleur qui assure le rôle de portail captif
- Des bornes (ou points d'accès) alimentées via des injecteurs
- Deux SSID sont disponibles :
  - o SSID à destination des collaborateurs du CTLes (Sécurisation par clé WPA)
  - o SSID à destination des invités (Sécurisation clé WPA)



### 2.2.2.3 Infrastructures WAN

Le routeur CTLes, infogéré par l'UGE assure les rôles suivants :

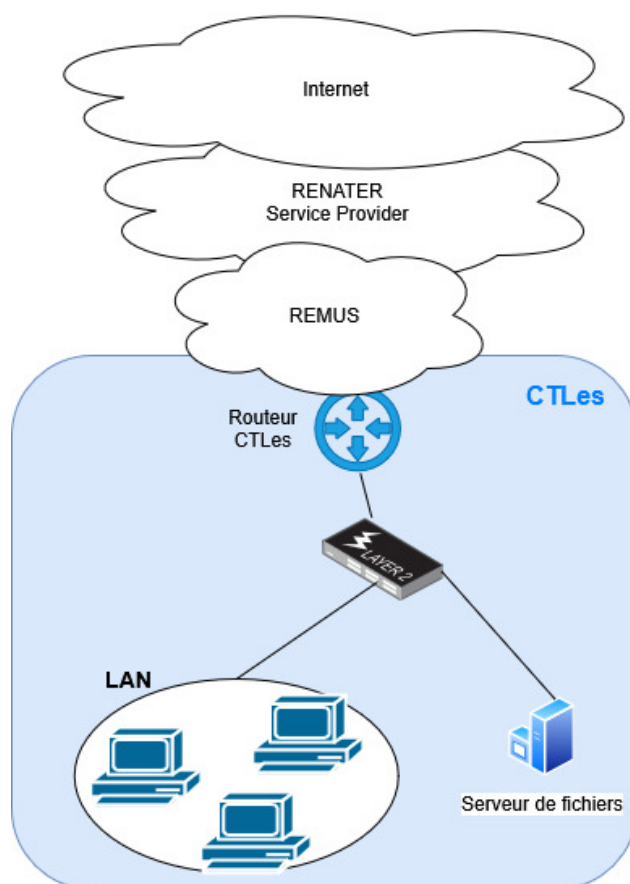
- Routage inter-vlan
- Filtrage<sup>3</sup>
- Passerelle vpn site à site

#### Accès à Internet et à Renater

Le schéma de la Figure 1 « Existant – Architecture de principe », présente l'existant au moment de la rédaction.

Dans le cadre des travaux préparatoires à la fin de la prestation d'infogérance de l'UGE, une évolution de l'architecture devra être effectuée.

Un des scénarios envisagés est le suivant : Le CTLes dispose de son propre accès à Renater et ainsi qu'à Internet. Le schéma ci-après présente l'architecture de principe envisagée



<sup>3</sup> Le filtrage principal est effectué par les équipements de l'université

### Accès à distance

L'accès à distance, notamment pour les collaborateurs en télétravail s'effectue via une passerelle VPN hébergée et infogérée par l'UGE.

L'accès distant s'effectue via l'application Wireguard. Un tunnel est monté entre le poste de travail du collaborateur et une passerelle VPN de l'Université. Ce tunnel permet de se connecter en mode bureau à distance au poste de travail fixe

#### 2.2.2.4 Infrastructures systèmes

Le CTLes héberge dans ses locaux un serveur physique. Ce serveur assure les rôles suivants :

- Serveur DHCP
- Serveur de fichier (Partage SMB)
- Gestion des comptes via l'interface Webmin

Caractéristiques du serveur :

- Hyperviseur Proxmox v7.1
- OS VM Debian

Le volume des données sur le serveur est de 2 To

Nota : L'Université Gustave Eiffel héberge l'infrastructure qui permet de s'authentifier sur le réseau Renater. Compte tenu des travaux prévus pour disposer d'un accès « direct » à Renater, ces serveurs d'authentification ne seront pas repris dans le cadre de la prestation d'infogérance, objet du présent CCTP.

### 2.2.3 Infrastructures techniques

Les bureaux du CTLes se situent à Bussy Saint-Georges sur un site partagé avec la BnF. La BnF assure la maintenance technique de l'ensemble des locaux du site.

La BnF effectue mensuellement un test électrique.

Ce test entraîne une coupure électrique d'environ 1h hors heures ouvrées.

## 2.3 Applications et services

### 2.3.1 Applications métiers

Le CTLes accède à trois types d'applications / services :

- des applications métiers SaaS
- des applications disponibles sur Renater ou le RIE
- le serveur de fichiers hébergé au CTLes

### Applications SaaS du CTLes

Les applications SaaS sont hors périmètre de la prestation d'infogérance, objet du présent CCTP

## Applications Renater utilisées par le CTLes

- Antispam personnalisable (<https://services.renater.fr/antispam/index>)
- Partage (<https://services.renater.fr/partage/index>)
- Universalistes (<https://services.renater.fr/groupware/universalistes/index>)
- Filesender, le transfert sécurisé de fichiers volumineux (<https://services.renater.fr/groupware/filesender/index>)
- Evento (<https://www.renater.fr/services/collaborer-simplement/evento>)
- Rendez-vous (<https://www.renater.fr/services/collaborer-simplement/rendez-vous/>)

## Services hébergés aux CTLes

Le CTLes héberge un serveur utilisé principalement comme serveur de fichiers tel que précisé au §2.2.2.4.

Ce serveur est accessible en interne mais également en télétravail via un vpn.

### 2.3.2 Logiciels

Outre les applications métiers, les postes de travail disposent des principaux logiciels suivants :

- Microsoft Office
- Client de messagerie Thunderbird
- Navigateur firefox
- Adobe pdf selon le collaborateur licence « reader » ou « professionnel »
- WinIBW : logiciel métier

Nota : au moins 1 collaborateur dispose d'une licence Photoshop

## 2.4 Autres

### 2.4.1 Nom de domaine

Le CTLes dispose de son nom de domaine : ctles.fr

Le renouvellement est automatique, et a priori, géré par Renater.

## 2.5 Infogérance actuelle : services et statistiques

### 2.5.1 Services actuels d'infogérance

L'Université Gustave Eiffel assure une prestation d'infogérance pour le CTLes

Le détail des services actuels est présenté en annexe 1 du présent document.

### 2.5.2 Statistiques des demandes et des incidents

Sur une période de 12 mois, le CTLes a fait appel à l'UGE pour différents types de demandes :

- Incidents : dysfonctionnement ou bug logiciel
- Demande de prestations : Modification de la configuration, Installation équipements, Création compte
- Demande d'évolution : Conseil pour le choix d'un équipement ou pour une étude d'évolution

Le tableau ci-dessous liste la répartition des demandes et les volumétries associées :

Catégorie	Type de demande (incident/accompagnement)	Volumétrie
Réseau	Incidents	8
	Demande de prestations	6
Messagerie (Partage)	Incidents	4
	Demande de prestations	6
Matériel	Incidents	3
	Demande de prestations	3
	Demande d'évolution	2

## 3 Prestations attendues

### 3.1 Prestations à l'initialisation du marché

Une phase d'initialisation est prévue en amont du démarrage effectif de la prestation d'infogérance.

Cette phase a pour objectif de permettre au titulaire :

- D'acquérir les connaissances et le savoir-faire nécessaires à l'exécution de l'ensemble des prestations d'infogérance prévues ;
- De mettre en œuvre les outils et méthodes nécessaires au pilotage et à l'exécution des prestations ;
- De prendre en charge les installations, systèmes, réseaux et services existants, sans interruption de service ni dégradation des niveaux de qualité attendus.

À l'issue de cette période, la responsabilité complète du système d'information et des réseaux est transférée au titulaire. Ce transfert donne lieu à un procès-verbal (PV) de transition, signé conjointement, marquant le passage à la phase opérationnelle.

Cette phase d'initialisation comprend notamment les activités suivantes :

**1. Etat des lieux :**

- Réalisation, en interaction avec la CTLes sur la base du document existant, de l'inventaire complet du système d'information, des réseaux, du matériel à maintenir, des logiciels et protocoles actifs ;
- Audit des configurations existantes, des équipements, des réseaux et de la sécurité associée ;
- Étude de l'architecture générale du système d'information et des réseaux, incluant les interconnexions, dépendances et points de vigilance ;
- À l'issue de cet état des lieux, le titulaire remet au CTLes un rapport détaillé d'état des lieux, incluant :
  - L'analyse de l'existant,
  - Les points faibles
  - Les recommandations d'optimisation ou de sécurisation,
  - Le plan d'action éventuel.

**2. Planification et préparation opérationnelle :**

- Définition et mise en place du cadre méthodologique de gestion de la prestation, incluant les outils de pilotage, le reporting et le suivi d'indicateurs ;
- Élaboration du planning prévisionnel des actions à venir (maintenances, évolutions, réunions de suivi) ;
- Définition des processus opérationnels (incident, demande, changement, gestion des vulnérabilité et processus d'escalade)

Cette phase d'initialisation du marché doit être réalisée en totalité en respect de la date de fin de la convention avec l'UGE prévue au 01/01/2026.

Le CTLes sera fermé entre 25 décembre 2025 et le 1<sup>er</sup> janvier 2026.

**CDRT1.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, ses références d'infogérance et le cas échéant des références dans des environnements semblables au CTLes.

**CDRT2.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, sa méthodologie d'initialisation du marché et le planning associé.

**CDRT3.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, le périmètre de l'état des lieux qu'il prévoit d'effectuer lors de la phase d'initialisation de la concession

## 3.2 Prestations initiales

### 3.2.1 Sauvegarde

Le titulaire est responsable de la fourniture et de la mise en œuvre d'une solution de sauvegarde.

#### Périmètre de la prestation :

- Données et environnements des systèmes

Le titulaire doit :

- Fournir une solution de sauvegarde adaptée au plan qu'il envisage et évolutive pour prendre en compte les éléments du paragraphe 3.3.5, Effectuer à une fréquence régulière des sauvegardes des données, des configurations, environnements, etc.
- Mettre en œuvre et configurer la solution de sauvegarde

La solution permet une résilience aux menaces suivantes : Chiffrement du SI, destruction partielle ou totale des locaux du CTLes, défaillance du système de sauvegarde.

La solution est évolutive et répond aux bonnes pratiques de sauvegarde.

Au démarrage de la prestation, la solution est dimensionnée pour permettre :

- La sauvegarde complète de l'environnement et des données du serveur
- Une rétention des sauvegardes sur 6 mois
- RPO : 24h

**CDRT4.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, sa solution de sauvegarde et ses processus de sauvegarde et de restauration. Il précise comment sa solution est résiliente face aux menaces cyber.

### 3.2.2 Sécurisation des flux internet et accès à distance

Le trafic réseau en provenance et à destination du système du CTLes doit faire l'objet d'un contrôle permanent afin de n'autoriser que les flux légitimes.

Le titulaire doit :

- Fournir, installer et configurer une solution pour sécuriser les flux vers et depuis internet.
- Fournir, installer et configurer une solution pour l'accès à distance aux SI du CTLes.

La solution de sécurisation des flux dispose, a minima, des fonctionnalités suivantes :

- Contrôle des flux entrés/sortis par IP, port, protocole et application
- Détection et prévention des intrusions (IDS/IPS) et protection contre les attaques par déni de service (DoS/DDoS) au niveau réseau
- L'inspection TLS
- Filtage URL web avec catégorisation et blocage des sites malveillants
- Mécanismes de notification en temps réel sur détection d'anomalies ou de violations de politiques

**CDRT5.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, la solution qu'il propose pour la sécurisation des flux. Il liste les fonctionnalités de la solution et indique le modèle financier associé.

**CDRT6.** Le soumissionnaire indique, dans le cadre de réponse prévu à cet effet, si la solution qu'il propose permet de gérer également le filtrage est-ouest.

Le titulaire doit fournir une solution sécurisée permettant l'accès en mobilité (principalement en télétravail) au SI du CTLes :

- Données hébergées sur des serveurs
- Applications Renater et RIE
- Application SaaS accessible à partir de l'adresse IP du CTLes

**CDRT7.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, les outils et/ou la solution qu'il compte déployer pour assurer l'accès en mobilité. Il présente sa méthodologie de mise en œuvre.

### 3.3 Les prestations de base

Le CTLes définit comme prestations de base, les prestations minimales fournies par le titulaire.

#### 3.3.1 Gestion du parc informatique

Le titulaire est responsable de la gestion et du maintien en conditions opérationnelles du parc informatique.

**Périmètre de la prestation :**

- Postes de travail (PC fixes et portables) et Serveurs
- Equipements réseaux (Routeur, switch, contrôleur wifi et bornes) et de sécurité
- Systèmes d'exploitation et logiciels de base (OS, outils bureautiques, clients de messagerie, etc.) ;

Le titulaire doit :

- Prendre connaissance de l'inventaire du parc informatique, et, si nécessaire, le mettre à jour. L'inventaire est disponible à la demande sous format électronique structuré (exportable .CSV, .XLSX);
- Procéder à l'installation, la configuration et la mise à jour des équipements et logiciels
  - o En s'appuyant notamment sur des solutions de type Master pour la préparation des postes de travail,
  - o En incluant la prise en charge des pilotes et logiciels des périphériques (imprimantes, webcams, etc.) ;
- Faire évoluer le master dans le cadre d'évolutions mineures (mises à jour de sécurité, nouveaux logiciels, modifications de configurations, etc.) ;
- Administrer les serveurs, équipements réseaux et de sécurité
- Réaliser une maintenance préventive et corrective : gestion des incidents, suivi des pannes, réparations et remplacements ;
  - o Les interventions s'effectuent sur site ou à distance ;
- Assurer une veille continue sur l'état du parc et formuler des préconisations claires en matière de :
  - o Renouvellement du matériel obsolète ou sous-performant ;
  - o Reconditionnement éventuel de certains équipements selon leur état et leur usage ;
  - o Mise au rebut sécurisée et traçable des équipements hors d'usage, incluant les procédures d'effacement sécurisé des données et/ou destruction du support de stockage et de recyclage.
- Sauvegarder les configurations des équipements réseaux et de sécurité

**CDRT8.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, le processus de gestion des entrées et sorties des collaborateurs. Le processus doit intégrer :

- La gestion de l'inventaire
- La gestion des accès
- La gestion du matériel (réaffectation du postes, suppression des données, ...)

Il présente les prérequis nécessaires à la réalisation de cette prestation (délai de notification pour la configuration du matériel et pour la gestion des accès, ...)

**CDRT9.** Le soumissionnaire présente, dans le cadre de réponse prévu à cet effet, sa méthodologie de mise à jour des masters.

### 3.3.2 Gestion des applications

Le titulaire accompagne et conseille le CTLes dans l'administration et la supervision des applications



**Périmètre de la prestation :**

- Services Renater : principalement la messagerie « Partage » et la gestion des identités « Identitas »
- Autres applications (client lourd) installées sur le poste de travail

Le titulaire doit :

- Assister le CTLes dans l'administration des services Renater, notamment la messagerie (création, modification ou suppression de comptes, récupération des BAL)
- S'assurer du bon fonctionnement des applications (client lourd) sur les postes de travail
- Effectuer un premier diagnostic en cas de dysfonctionnement (avant une éventuelle escalade technique)
- Intervenir en lieu et place du CTLes lorsque les opérations requièrent un niveau d'expertise technique (supérieur aux compétences internes)

**CDRT10.** Le soumissionnaire décrit, dans le cadre de réponse prévu à cet effet, sa connaissance des applications Renater et précise ses références

### 3.3.3 Gestion de nom de domaine

Le titulaire accompagne le CTLes dans la bonne gestion administrative, technique et sécuritaire des noms de domaine.

**Le périmètre de la prestation :**

- L'enregistrement
- Le renouvellement
- Le transfert éventuel

Le titulaire accompagne, éventuellement, le CTLes à :

- L'acquisition de nouveaux noms de domaine et leur renouvellement à échéance sans interruption de service.
- La gestion et les mises à jour des enregistrements DNS

**CDRT11.** Le soumissionnaire indique, dans le cadre de réponse prévu à cet effet, sa capacité à accompagner le CTLes pour la gestion des DNS.

### 3.3.4 Sécurité du SI

Le titulaire est responsable du Maintien en Conditions de Sécurité (MCS) de l'ensemble des composants relevant du périmètre de la prestation, notamment :

- Les serveurs physiques et virtuels, ainsi que les systèmes d'exploitation et services associés ;
- Les équipements réseaux (switch, routeur, point d'accès, firewall, etc.) ;
- Les équipements et dispositifs de sécurité

Le Maintien en Conditions de Sécurité a pour objectif de :

- Assurer la sécurité des systèmes d'information ;
- Réduire les risques liés aux vulnérabilités, aux intrusions et aux comportements anormaux ;
- Contrôler et maîtriser les flux réseau internes et externes ;

Pour se faire, le titulaire effectue, a minima, les actions suivantes :

- Segmentation et sécurisation des flux internes et externes ;
- Application des correctifs de sécurité (patches) en fonction de leur criticité, selon un processus validé ;
- Surveillance continue des journaux, alertes, comportements anormaux et vulnérabilités potentielles ;
- Analyse régulière des journaux d'événements ;
- Revue périodique des règles de filtrage ;
- Traçabilité et archivage des opérations liées à la sécurité.

#### **3.3.4.1 Anti-malware**

Le titulaire est responsable de la sécurisation du parc informatique et des serveurs<sup>4</sup>.

Le titulaire doit :

- S'assurer que la protection antimalware est effective sur l'ensemble du parc informatique.
- Analyser les alertes issues des outils anti-malware

#### **3.3.4.2 Gestion des vulnérabilités**

Le titulaire est responsable de la détection, de l'analyse, du suivi et du traitement des vulnérabilités.

**Le périmètre de la prestation :**

- Postes de travail (PC fixes et portables) et Serveurs
- Equipements réseaux (Routeur, switch, contrôleur wifi et bornes) et de sécurité
- Systèmes d'exploitation et logiciels de base (OS, outils bureautiques, clients de messagerie, etc.) ;

Le titulaire doit mettre en œuvre un processus formel de gestion des vulnérabilités aligné avec les bonnes pratiques. Ce processus intègre :

- La réalisation d'une surveillance proactive des vulnérabilités
- L'évaluation de la criticité des vulnérabilités dans le contexte du CTLe
- La proposition de plans de remédiation

---

<sup>4</sup> Eventuellement, au démarrage de la prestation, reprise de la solution anti-malware existante

**CDRT12.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, son processus de gestion des vulnérabilités, son processus de notification et d'escalade en cas de vulnérabilité majeur et son processus de patch management.

### **3.3.4.3 Journaux d'évènements**

Le titulaire est responsable de la mise en place, de la collecte, de la conservation, et de l'exploitation des journaux d'événements générés par les systèmes, équipements et applications inclus dans le périmètre d'infogérance.

#### **Le périmètre de la prestation :**

- Postes de travail (PC fixes et portables) et Serveurs
- Equipements réseaux (Routeur, switch, contrôleur wifi et bornes) et de sécurité
- Systèmes d'exploitation et logiciels de base (OS, outils bureautiques, clients de messagerie, etc.) ;

**CDRT13.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, son processus de gestion des journaux d'événements. Le type de journaux qu'il compte collecter (journaux d'accès, d'administration, ...), sa stratégie de collecte et de sauvegarde des journaux d'événements et la durée de conservation

**CDRT14.** Le soumissionnaire indique, dans le cadre de réponse prévu à cet effet, sa fréquence de revue des journaux.

### **3.3.5 Sauvegarde et restauration**

Le titulaire est responsable du suivi, de la vérification et de la restauration des sauvegardes des systèmes, données et configurations, afin de garantir la résilience des services et la capacité à restaurer les éléments critiques en cas d'incident.

#### **Périmètre de la prestation :**

- Données et environnements des systèmes

Le titulaire doit :

- Effectuer à une fréquence régulière des sauvegardes des données, des configurations, environnements, etc.
- Effectuer à une fréquence régulière des tests de restauration. Sur une période donnée, le titulaire aura effectué des tests de restauration sur l'ensemble du périmètre.
- Vérifier quotidiennement l'intégrité et le bon déroulement des sauvegardes et notifier en cas d'échec ou d'anomalie.
- Être en mesure de restaurer les données ou systèmes si besoin

**CDRT15.** Le soumissionnaire présente, dans le cadre de réponse prévu à cet effet, le plan de sauvegarde qu'il préconise et les délais de restauration. Il précise à minima les éléments suivants : le type, la fréquence et la rétention

### 3.3.6 Monitoring (surveillance opérationnelle et de sécurité) du parc

Le titulaire effectue une surveillance opérationnelle et de sécurité du parc.

#### Périmètre de la prestation :

- PC et Serveurs
- Equipements réseaux et de sécurité

Le titulaire doit :

- Surveiller en temps réel l'état de fonctionnement des serveurs (physiques et virtuels), des équipements réseau et des équipements de sécurité permettant :
  - o La détection automatique des anomalies, pannes, dépassements de seuils
  - o L'émission d'alertes selon des règles définies (pendant la phase d'initialisation) ;
- Surveiller en temps réel le niveau de sécurité des PCs, des serveurs (physiques et virtuels), des équipements réseaux et des équipements de sécurité permettant :
  - o La détection automatique de comportements ou situations anormales
  - o La notification en quasi-temps réel et prise en charge sans délai selon la gravité de l'évènement.
- Collecter les indicateurs de performance tels que :
  - o La disponibilité, la bande passante entrante et sortante pour l'accès à internet
  - o Le CPU, la RAM, la capacité de stockage, etc. des serveurs
  - o La disponibilité des équipements
- Collecter les indicateurs de violation des politiques de sécurité
- Eventuellement collecter les indicateurs de compromission

Ces éléments sont accessibles à la demande par le CTLes.

**CDRT16.** Le soumissionnaire précise, dans le cadre de réponse prévu à cet effet :

- Les outils qu'il compte mettre en place pour assurer le monitoring.
- Sa capacité à fournir un accès en temps réel aux outils de monitoring au CTLes
- Sa capacité à personnaliser les notifications en cas de dépassement de seuil et/ou comportement anormal

### 3.3.7 Gestion des incidents et des demandes

#### 3.3.7.1 Gestion des incidents

Le titulaire est responsable de la gestion des incidents, selon la terminologie suivante :

- Incident : événement ne faisant pas partie du fonctionnement normal d'un service (ou d'un équipement) et causant ou pouvant causer une interruption non prévue d'un service informatique ou une réduction de sa qualité.
- Incident de sécurité : événement compromettant ou pouvant compromettre la confidentialité, l'intégrité et/ou la disponibilité des données
- Résolution d'un incident : retour au fonctionnement normal du service via une solution pérenne.

**Périmètre de la prestation :**

		Niveau 0	Niveau 1	Niveau 2
		Prise en compte de l'incident	Traitement des incidents simples (procédure de résolution connue)	les actions du niveau 1 n'ont pas permis de résoudre l'incident, ou Nouveau incident / complexe
Matériel (et OS le cas échéant)	Terminaux	CTLes	CTLes	Infogérant
	Serveurs		Infogérant	
	Petits périphériques		Infogérant - réinstallation de pilotes	Infogérant : Logiciel Editeurs : Matériel
Logiciels et Services	Applications SaaS		CTLes	Editeurs
	Applications Renater		Infogérant	Renater
	Applications / services hébergés		CTLes : Gestion des comptes Infogérant : Logiciel	Infogérant
Connectivité	Accès à Internet		CTLes	Infogérant
	Réseau local (filaire et sans fil)	Infogérant	Infogérant	Infogérant
Sécurité	Infogérant		Infogérant	

## Niveaux de service attendus

Gestion des incidents	Criticité	Description	Délai de prise en charge	GTR
	Critique	Un incident est considéré comme critique dès que 50 % des collaborateurs rencontrent des difficultés (indisponibilité totale ou instabilité prolongée) pour se connecter aux applications métiers (locales et/ou externes). <u>Exemples :</u> <ul style="list-style-type: none"> <li>- Perte de l'accès à Internet</li> <li>- Défaillance du FW</li> <li>- Défaillance des équipements réseaux</li> <li>- Défaillance du serveur</li> </ul>	1 h	4h – HO
	Majeur	Un incident est considéré comme majeur lorsqu'il pénalise un nombre restreint de collaborateurs ou qu'il concerne 1 outil / application : <u>Exemples :</u> <ul style="list-style-type: none"> <li>- Panne de 1 PC</li> <li>- Anomalie sur les outils bureautiques</li> <li>- Panne de l'accès en mobilité (si collaborateurs impactés &lt; 50 % du personnel)</li> <li>- Panne de la sauvegarde</li> </ul>	2 heures	2j – JO
	Mineur	Les autres incidents, dysfonctionnements et anomalies sont considérés comme des mineurs	4 heures	5j – JO

**CDRT17.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, son processus de gestion des incidents. Il précise ses processus d'escalade managériale et technique.

**CDRT18.** Le soumissionnaire confirme, dans le cadre de réponse prévu à cet effet, sa capacité à respecter les SLA indiqués dans le tableau ci-dessus.

### 3.3.7.2 Gestion des demandes

Le titulaire est responsable de la gestion des demandes. Le CTLes identifie 2 types de demande :

- Demande de prestations
  - Ces demandes sont décrites dans le §3.4.1 – Demande de prestation.
- Demande de conseil ou d'évolution mineure :
  - Conseil pour le choix d'un équipement ou pour une étude d'évolution, ajout d'une nouvelle règle firewall (FW), changement d'une borne, accompagnement à la validation d'un devis matériel, choix de matériel actif ou passif, gestion du MFA sans téléphone professionnel, etc.
  - Assistance dans les discussions techniques avec d'autres fournisseurs du CTLes. Ex : Opérateur, Renater, éditeurs, ...

#### Niveaux de service attendus

Gestion des demandes	Type	Description	Délai de prise en charge	GTR (en heures ouvrable HO ou jours ouvrables JO)
	Urgente	Une requête ou un besoin qui nécessite une attention immédiate.	1h	4h – HO
	Standard	Une requête à faible risque Ex. demande de conseil	2h	5J – JO

**CDRT19.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, son processus de gestion des demandes de conseil et d'évolution mineure.

**CDRT20.** Le soumissionnaire confirme, dans le cadre de réponse prévu à cet effet, sa capacité à respecter les SLA indiqués dans le tableau ci-dessus

### 3.3.7.3 Modalités et horaires d'intervention

Le titulaire doit :

- Fournir les moyens de communication nécessaires pour déclarer un incident, faire une demande et suivre les traitements
  - La déclaration ou l'émission d'une demande est possible 7j/7 et 24h/24
  - Une plateforme permet de
    - Tracer chaque demande
    - Suivre les durées de prises en charge et de traitement
    - D'établir des statistiques, a minima, mensuelles sur les incidents et les demandes
- Assurer le support aux utilisateurs du lundi au vendredi de 8h à 18h. L'assistance est effectuée à distance ou sur site
  - Assistance sur site si besoin
  - Escalade vers le niveau 3 ou les éditeurs si nécessaire

- Traiter les incidents et demandes selon leur niveau de criticité
- Mettre en œuvre une solution de contournement, dans les cas où une résolution de l'incident n'est pas possible ou validée.
- Appliquer un processus d'escalade technique et organisationnel prédéfini
- Analyser les causes racines des incidents critiques et majeurs de sécurité

### 3.4 Prestations complémentaires

#### 3.4.1 Demande de prestations

Les demandes de prestations correspondent à :

- Une maîtrise d'œuvre spécifique pour toute opération d'envergure ou d'incidence majeure sur le Système d'Information, qu'elle soit initiée par le CTLes ou le titulaire (par exemple : évolution majeure de l'architecture réseaux et système).
- Des demandes d'interventions dans le cadre des missions prévues au présent marché mais en dehors des heures de service normales.

Pour les demandes de prestation, le titulaire doit :

- Réaliser une analyse d'impact technique et organisationnel
- Présenter les changements envisagés au CTLes
- Planifier le changement en concertation avec le CTLes en s'assurant de sa réversibilité en cas d'échec.
- Réaliser des tests de vérification d'aptitude post-changement.
- Mettre à jour les documents d'architecture et d'exploitation après mise en production.

Ces demandes de prestation sont rémunérées sur la base d'une proposition établie par le titulaire en fonction des tarifs définis dans le bordereau des prix unitaires.

Toute prestation de ce type donnera lieu à une étude préalable réalisée par le titulaire pour évaluer le budget nécessaire et la charge de travail incombant à chacune des parties (titulaire et CTLes). Cette étude préalable **est comprise dans les prestations de base**.

**CDRT21.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, son processus de gestion des demandes de prestation et les délais sur lequel il s'engage pour chaque étape de son processus.

**CDRT22.** Le soumissionnaire indique, dans le cadre de réponse prévu à cet effet, les critères ou la méthode qu'il utilise pour distinguer les demandes de conseil incluses dans la prestation de base (demande de conseil) de celles donnant lieu à une facturation complémentaire.



### 3.4.2 Anti-malware

En complément de la prestation décrite dans le paragraphe 3.2.4, le titulaire, à la demande, fournit et déploie sur l'ensemble du parc (PCs et Serveur) une solution anti-malware avancée.

La solution mise en œuvre doit intégrer, a minima, les fonctionnalités suivantes :

- Détection et neutralisation des virus, trojans, ransomwares et spywares.
- Protection contre les scripts malveillants (PowerShell, JavaScript, macros).
- Gestion centralisée de la solution (console d'administration).
- Reporting et alerting personnalisables.
- Mise en quarantaine de l'équipement infecté.

**CDRT23.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, la solution antimalware qu'il propose. Il présente les atouts de sa solution et les points faibles

### 3.4.3 Création et déploiement d'un master

Au démarrage (dans les premiers mois) de la prestation, le titulaire construit et déploie un nouveau master pour les postes de travail du CTLes.

Le master comprend a minima, les logiciels existants.

Ce master repose sur la dernière version patchée du système d'exploitation Windows 11 et doit être déployé sur l'ensemble des postes du parc (Actif et en stock).

A date, le parc devrait être composé d'environ 70 postes de travail.

20 à 30% des 70 postes seront à remplacer lors du déploiement du nouveau master (ces postes sont actuellement en stock).

**CDRT24.** Le soumissionnaire présente sa méthodologie pour la création du nouveau master et le déploiement sur le parc existant

### 3.4.4 Evolution majeure du master

Le CTLes définit l'évolution majeure du master comme une modification significative du système (Exemple : changement de version du système d'exploitation.)

Les évolutions majeures seront traitées dans le cadre de demande de prestation avec un devis associé sur la base des unités d'œuvre du BPU (cf. Partie « Divers » du document « BPU »).

### 3.4.5 Installation d'un nouveau poste de travail

Cette prestation vise à configurer et installer un nouveau poste de travail à partir d'un équipement neuf fourni par le CTLe.

Elle intègre notamment :

- La maîtrise du poste
- L'intégration du poste dans le parc
- Le paramétrage réseau
- La configuration de l'accès distant
- Etc.

A l'issue de la prestation, le poste est prêt pour une utilisation par le collaborateur

Nota : Cette prestation s'applique en phase d'exploitation (Elle ne s'applique pas lors du déploiement initial du nouveau master – cf. Paragraphe 3.4.3).

**CDRT25.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, sa méthodologie de configuration et d'installation d'un nouveau poste de travail. Il détaille ses étapes, et présente les prérequis et les limites.

### 3.4.6 Evolution de l'infrastructure locale

Le titulaire fournit, installe et configure une nouvelle solution pour répondre aux besoins couverts par l'actuel serveur local (cf. §2.1.2) afin de palier à l'obsolescence du serveur.

**CDRT26.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, sa solution pour la reprise des services hébergés sur le serveur. Il présente les limites de sa solution.

## 3.5 Documentation

Le titulaire s'engage à tenir à disposition du CTLe des documents et schémas d'architecture à jour. La documentation est claire et rédigée en français, structurée et accessible, permettant au CTLe de comprendre, suivre et reprendre la gestion des systèmes et services en cas de besoin.

À ce titre, le titulaire doit :

- Stocker la documentation dans un espace de stockage unique accessible par le CTLe.
- Rédiger et maintenir à jour les documents suivants :
  - o Inventaire des actifs tels que précisé dans la prestation de gestion du parc informatique (§3.2.1)
  - o Un Dossier d'architecture technique (plan d'adressage, équipements actifs, liens, filtrage).
  - o Procédures courantes (sauvegarde/restauration, redémarrage serveurs/services, installation de logiciels).
- Mettre à jour la documentation dans un délai maximal de 5 jours ouvrés après tout changement majeur ayant un impact sur la documentation.

**CDRT27.** Le soumissionnaire indique, dans le cadre de réponse prévu à cet effet, comment il partage la documentation avec le CTLes

## 3.6 Organisation de la prestation

### 3.6.1 Interlocuteurs de référence

Le titulaire s'engage à mettre à disposition un interlocuteur de référence (ou un couple d'interlocuteurs) pendant toute la durée du marché. Les interlocuteurs maîtrisent les dimensions commerciales et technique du marché

**CDRT28.** Le soumissionnaire indique, dans le cadre de réponse prévu à cet effet, l'organisation qu'il envisage

### 3.6.2 Comitologie : phase mise en œuvre initiale

**CDRT29.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, la gouvernance qu'il mettra en place pendant la phase de mise en œuvre initiale. Il précise :

- les thématiques qui seront abordées
- le type et la fréquence des réunions

### 3.6.3 Comitologie : phase d'exploitation

Le CTLes souhaite la tenue de réunions de suivi du marché selon une fréquence ci-dessous :

- Mensuelle pendant les 6 premiers mois de la prestation
- Trimestrielle à partir du 7<sup>ème</sup> mois

Cette fréquence pouvant être amenée à évoluer suivant la criticité des points ou à la demande en cas de situation exceptionnelle.

Le comité de pilotage sera composé :

- Pour le CTLes: du Directeur, et de toute autre personne invitée en fonction des sujets traités ;
- Pour le Titulaire : du responsable de suivi du compte, et de toute autre personne invitée en fonction des sujets traités.

Le rôle et les missions du comité de pilotage sont les suivants :

- Dresser le bilan d'exploitation et suivre les indicateurs de performance sur la période écoulée comportant :
  - o Rapport des incidents et des vulnérabilités
  - o Etat des sauvegardes et des tests de restauration réalisés et les éventuelles non-conformités
  - o Demande de prestations traitée et en cours
  - o Analyser la qualité des prestations, étudier les propositions d'actions correctives du titulaire et décider de leur mise en œuvre
- Présenter ses nouvelles orientations stratégiques

Chaque réunion du comité de pilotage doit faire l'objet d'un compte rendu rédigé par le titulaire.

**CDRT30.** Le soumissionnaire détaille, dans le cadre de réponse prévu à cet effet, la comitologie qu'il propose pendant la phase d'exploitation

### **3.7 Mise en œuvre**

#### **3.7.1 Architecture**

**CDRT31.** Le soumissionnaire décrit, dans le cadre de réponse prévu à cet effet, l'architecture cible qu'il envisage pour traiter dès le démarrage de la prestation :

- L'accès à distance
- La sécurisation des flux
- La sauvegarde et restauration

**CDRT32.** Le soumissionnaire présente, dans le cadre de réponse prévu à cet effet, une variante de l'architecture cible. Cette variante intègre l'évolution de l'infrastructure serveur (§3.3.7)

#### **3.7.2 Méthodologie et organisation**

**CDRT33.** Le soumissionnaire présente, dans le cadre de réponse prévu à cet effet, sa méthodologie de mise en œuvre pour assurer la continuité des services. Il détaille les moyens organisationnels, humains et techniques qu'il prévoit de mobiliser, ainsi que les mesures qu'il envisage pour garantir la disponibilité des services.

#### **3.7.3 Planning de mise en œuvre**

Il est rappelé que **la prestation d'infogérance pour le CTLes est attendue à partir du 1<sup>er</sup> janvier 2026.**

**CDRT34.** Le soumissionnaire propose, dans le cadre de réponse prévu à cet effet, un planning prévisionnel pour la reprise des services et la mise en œuvre de l'architecture cible qu'il envisage, en prenant en compte toutes les prestations initiales (§3.2) et de bases (§3.3)

**CDRT35.** Le soumissionnaire présente, dans le cadre de réponse prévu à cet effet, une seconde version de son planning prévisionnel dans lequel il intègre en complément des prestations listées dans le CDRT30, l'évolution de l'infrastructure serveur (§3.3.7)

Nota : le soumissionnaire précise dans ses plannings prévisionnels, les prérequis techniques et temporels (ex : échéance pour la fourniture de l'accès à Internet) pour le respect de son planning.

### **3.8 Vérification d'aptitude (VA), Vérification de service régulier (VSR)**

Dans le cadre du contrôle de la qualité de la prestation, le titulaire organise des vérifications systématiques afin de valider le bon fonctionnement des services délivrés et leur conformité aux exigences du CTLe.

#### **3.8.1 Vérification d'Aptitude (VA)**

La VA est réalisée à la mise en production initiale du service, ou lors de la livraison d'un composant majeur (nouvelle solution, infrastructure, ou évolution importante).

À ce titre, le titulaire doit :

- Présenter un plan de tests fonctionnels et techniques
- Documenter les résultats et lever les éventuelles réserves dans un délai convenu.
- Obtenir la validation formelle du client avant passage en exploitation courante.

#### **3.8.2 Vérification de Service Régulier (VSR)**

À l'issue positive de la vérification d'aptitude, les services seront réputés en production et feront l'objet d'une période de suivi de fonctionnement en service régulier qui aura une durée de 1 mois.

Au cours de la période de VSR, au fur et à mesure de ses observations, le CTLe transmettra ses relevés d'anomalies.

Des réunions périodiques seront organisées par le CTLe et le responsable côté titulaire pour répondre aux demandes de corrections éventuelles mais aussi sur l'avancement des corrections attendues.

La VSR pourra être ajournée ou rejetée en cas de :

- Panne entraînant une indisponibilité totale des services de plus de 4 heures ouvrées (Ex. : panne de la solution de sécurisation des flux);
- Les délais de traitement des services exigés au présent CCTP ne sont pas respectés ;

À l'issue positive de cette période, et sur acceptation du dossier d'exploitation, le CTLe prononcera la réception des services d'infogérance.

### 3.9 Limites de la prestation

**CDRT36.** Le soumissionnaire présente, dans le cadre de réponse prévu à cet effet, les limites de sa prestation au regard des exigences et attentes du présent CCTP

L'acquisition du matériel informatique de type PC, Serveurs, équipements réseaux (hors routeurs et FW) et périphériques (Imprimantes, Webcam, etc.) ne fait pas partie de la prestation demandée.

### 3.10 Réversibilité et transférabilité

La phase de réversibilité / transférabilité a pour objectif d'assurer une migration en douceur en cas de reprise des services en interne ou de changement de titulaire au terme du marché et d'assurer le transfert des services.

Le titulaire devra une participation pleine et entière dans le cas où il ne serait pas attributaire du marché suivant.

Cette assistance comprend sans être exhaustif :

- La participation à toutes les réunions organisées sur site par le CTLes ;
- La participation à tous les échanges téléphoniques, mails etc. nécessaires ;
- La collaboration pleine et entière avec le ou le prestataire entrant afin d'assurer les processus de transfert des services ;

Le titulaire ne peut réclamer un quelconque dédommagement pour les services qui sont résiliés progressivement durant la phase de réversibilité / transférabilité. La durée de la phase de réversibilité / transférabilité est fixée par le CTLes, en fonction de l'engagement de délai de prise en charge du nouveau titulaire.

De plus, il assurera un support complet (échanges par mails, téléphones, etc.) afin de faciliter le plus possible les opérations techniques et administratives.

Si les services n'ont pas encore été résiliés, le titulaire ne peut s'opposer à une procédure de retour en arrière durant la phase de réversibilité / transférabilité notamment si le CTLes estime qu'il est impossible de migrer les nouveaux services vers le nouveau partenaire. Les prestations techniques nécessaires font partie du coût de la réversibilité / transférabilité.

À l'issue des opérations positives de réversibilité / transférabilité, les actions ci-dessous doivent être réalisées :

- sur ordre du CTLes, toutes les données stockées ou sauvegardées sur les infrastructures du Titulaire du présent marché devront être détruites ;
- Fourniture d'un PV de réception de transférabilité qui sera signé conjointement avec le CTLes, le Titulaire sortant et le Titulaire entrant.

**CDRT37.** Le soumissionnaire indique, dans le cadre de réponse prévu à cet effet, comment il assure la réversibilité ou transférabilité de ses services à la fin de sa prestation.

## 4 Développement durable / RSE

### 4.1 Développement durable

**CDRT38.** Le soumissionnaire, dans le cadre de réponse prévu à cet effet, décrit son action en matière de développement durable pour :

- Le choix des matériels et des composants
- La gestion des déchets électroniques

### 4.2 Responsabilité sociétale

**CDRT39.** Le soumissionnaire, dans le cadre de réponse prévu à cet effet, décrit son action en matière de responsabilité sociétale (conformité ISO 26000 ou équivalent). Il détaille notamment :

- Sa politique RSE
- Son plan d'action
- Ses processus
- Ses procédures
- Son activité d'amélioration continue

## **ANNEXE 1 PRESENTATION DES SERVICES ASSURES PAR L'UGE**

### **Services liés à l'accès et aux services Renater**

L'UGE installe et configure les matériels actifs (routeurs) nécessaires au raccordement du CTLes à la prise RENATER de l'UGE. Cette installation respecte les limites définies par le groupement d'intérêt Public RENATER.

L'UGE installe et configure les boîtes de messageries dans les limites définies par RENATER.

L'installation et le fonctionnement des matériels et logiciels nécessaires au raccordement du CTLes à Internet sont pris en charge par le CTLes (à titre d'exemple : contrat avec opérateur telecom ou équivalent, changement de matériel réseau). Les configurations techniques de la liaison VPN permettant la connexion du CTLes au réseau de l'UGE sont prises en charge par la DGDIN de l'UGE. Les matériels nécessaires à cette liaison sont achetés par le CTLes sur recommandation de la DGDIN.

L'Université Gustave Eiffel assure l'administration et la maintenance des outils réseaux, logiciels et matériels pour le compte du CTLes.

Le CTLes accède aux services suivants proposés par l'UGE :

- Proxy/cache web ;
- Serveur de temps ;
- L'installation, le paramétrage, l'administration et la maintenance d'un serveur VPN pour permettre les accès distants (télétravail, nomadisme)
- Hébergement du nom de domaine (DNS), déclaration des machines et des alias ;
- Serveur de messagerie au travers de la plateforme de messagerie collaborative « PARTAGE » de RENATER ;
- Services Antispam, antivirus ;
- Création et gestion de boîtes à lettres personnelles et impersonnelles. Les boîtes de messagerie utilisent le protocole IMAPS.
- Hébergement dans la salle machine de l'université de serveurs ou machine virtuelle

### **Assistance technique pour le parc micro-informatique**

- Conseils pour l'achat de matériel informatique (PC, serveur, imprimante, matériel réseau) ;
- Mise en place et administration d'un serveur de VPN ;
- Mise en place et l'exploitation d'un serveur d'authentification Shibboleth (IdP) intégré au sein de la fédération nationale portée par RENATER.
- Mise en place et administration d'un serveur de fichiers ;
- Configuration du réseau local : plan d'adressage, commutateurs, serveur DHCP ;
- Configuration, paramétrages du serveur de domaine ;
- Configuration, installation des machines clientes (préparation et déploiement de l'image Ghost) ;
- Configuration, installation et assistance d'un parc d'ordinateurs portables de télétravail ;
- Configuration, installation des imprimantes et copieurs ;
- Mise en place et administration d'une infrastructure de sauvegarde ;
- Mise en place d'une redondance de sauvegarde afin de sécuriser les données.

### **Détail concernant les processus de sécurité**



**Filtrage**

- En complément des règles de filtrage configurées sur le « routeur CTLes », l'Université propose également du filtrage de flux

**Antimalware**

- Windows Defender

**Sauvegarde**

- La sauvegarde des environnements et des données est réalisée par l'Université.
  - Le plan de sauvegarde du serveur local est le suivant :
    - o Sauvegarde différentielle toutes les nuits
    - o Une fois par semaine, l'Université réalise des snapshots des données des VMs
    - o Rétention des données sauvegardées : 6 mois
- L'Université se charge de la restauration des données

**Patch management**

- Linux : Les mises à jour du serveur CTLes sont réalisées à des fréquences irrégulières
- Windows (poste de travail) : via Windows update

**Journalisation des événements**

- Aucune centralisation des journaux d'événements n'est réalisée.