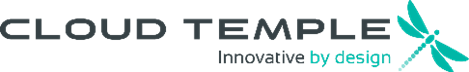
Convention de Service IaaS



Logo Cloud Temple

# 1. **CONVENTION DE SERVICES IaaS**

| **Destinataires :** | **COMMANDITAIRE** |
| --- | --- |
| **Référence du documents** | CT.AM.JUR.ANX - 20240403\_v2.0.docx\_Jour JJ AAAA |
| **Vos interlocuteurs** | *Prénom* *Nom* |
|  | Account Manager |
|  | e-mail : *prenom.nom*@cloud-temple.com |
| **Date de dernière mise à jour** | 03/04/2024 |
| **Date de validation contractuelle** | Jour JJ AAAA |

| **Version** | **Date** | **Action** | **Auteur** |
| --- | --- | --- | --- |
| v0.1 | 07/06/2022 | Rédaction initiale | Lorena ALCALDE |
| v0.2 | 14/09/2022 | Enrichissement | Lorena ALCALDE |
| v1.0 | 30/12/2022 | Intégration Indicateurs | Lorena ALCALDE |
| v1.1 | 23/01/2023 | Modification pied de page | Lorena ALCALDE |
| v1.2 | 22/05/2023 | Enrichissement | Lorena ALCALDE |
| v1.3 | 29/06/2023 | Enrichissement | Lorena ALCALDE |
| v1.4 | 06/11/2023 | Modification Capital et Enrichissement | Lorena ALCALDE |
| v1.5 | 30/11/2023 | Enrichissement | Lorena ALCALDE |
| v1.6 | 21/03/2024 | Enrichissement | Lorena ALCALDE |
| v2.0 | 29/03/2024 | Ajustements conformité SNC | Nicolas ABRIOUX |
| v2.0 | 03/04/2024 | Publication | Lorena ALCALDE |

# 2. **TABLE DES MATIÈRES**

* [1. **CONVENTION DE SERVICES IaaS**](#Xc3786c07943ae71dec5191b24567a7f31cb6100)
* [2. **TABLE DES MATIÈRES**](#X3dffd8c5466b60a9d1847f151e1ff8bf27d5bbe)
* [3. Préliminaire et Glossaire](#X9df3d46524e9acceada5b6725a4b3f19a8b9b42)
  + [3.1. Préliminaire](#X72bdbcbbf0c088c7b664a8859dff9c5e94a1c67)
  + [3.2. Glossaire](#X0bd89fddb7967cedd9680ed4f7efa236729ef3e)
* [4. Acronymes](#X69ea3329484b8f0083d344ad9c43d7dabdcccc9)
* [5. Objet de la présente Convention de service](#X30e34f28e133265489633a87e3abd4d1a022de5)
* [6. Audit](#X910e2801262de94af715f54b8fb509cc70cc79a)
* [7. Description du Service](#X3d12a6c93683f0122f5f9a8e21e7c12fc92490b)
  + [7.1. Modèle de responsabilité partagé](#X5ab2fd5cebb0dc76febf8e32f5665b447285437)
  + [7.2. Présentation détaillée du périmètre du Service](#Xd81ad0562f6e00e693916802084624b2a4885a5)
    - [7.2.1. Infrastructures Datacenters](#Xfd30a9e9ca5808eb0dd2b0f76d8755ff494726d)
    - [7.2.2. Infrastructure logicielle de pilotage du Service](#X429d709e167549b1f31f4cdbe79bbf526f0b1dc)
    - [7.2.3. Infrastructures de calcul](#X432e4596f65dd97ffb3314bc9725a08a9369f4d)
    - [7.2.4. Infrastructure de stockage](#X30efbac0441ad31cd6ec07282a96acfcd07e9b2)
    - [7.2.5. Infrastructure réseau globale](#X78b4484e386c95a988a698cd84bae342679ddb5)
    - [7.2.6. Infrastructure de sauvegarde](#Xdf2c99a6958ca2f79a1cf60659dd5a3029ab31c)
    - [7.2.7. Mise en œuvre de solutions de reprise d’activité ou de continuité d’activité](#X5610bffa77dd118e87cbee05f204158179c962f)
  + [7.3. Limitations des services dans le modèle IaaS qualifié](#X9afa960ae3673041349d17f6a264de8fb35d3b0)
    - [7.3.1. Services managés en RUN](#Xa64cd9832e1132b6d2d4e8ef50163a925fcceeb)
    - [7.3.2. Configuration du secours](#Xfc39a8474ae9c8d4eedbb3b8e543dc0a137bd71)
    - [7.3.3. Configuration de la sauvegarde](#Xfd8664b285a442773de0c9989256f92bc1f6ca2)
  + [7.4. Mise en œuvre du service](#X93e04903630a0a81d7b9ebc1a4c5a933dfa0088)
    - [7.4.1. Prérequis techniques](#X59ca4242dbed0e6d5e3efa2ba91a80866647f92)
  + [7.5. Localisation du service en France](#Xdcea3053acc96cf4c715a189f3d7d9842c70915)
    - [7.5.1. Localisation des Datacenters hébergeant le Service](#Xac9c0f685576284f9431d5c1b6df99bc7ab662b)
    - [7.5.2. Localisation des agences Cloud Temple opérant le service](#X528b4e5e85b084898df1a4b0ee003fda94dca5d)
  + [7.6. Support](#X451baaab9b4764d97da95395b7e24265143a283)
    - [7.6.1. Nature du support accompagnant le service](#X192381358bcad693baa22b16773742f4c8cf227)
    - [7.6.2. Sollicitation du service support technique](#X03ef425751011df1818d9488df5625576c33f5e)
    - [7.6.3. Processus de gestion des Incidents](#Xac759d2aee6d685130dea876d7a1ed03888b994)
    - [7.6.4. Processus de priorisation des traitements](#X30a0604e2d2957ae43d1f1fe2cb9c04f5c05885)
    - [7.6.5. Langue et localisation du service de support](#X1afc584a9d5f886a1ad8b9ca498773d2e10cff8)
* [8. Engagements et niveaux de services](#Xf1662fa601c14a35f4b238c1effe9c712d3efbe)
  + [8.1. Engagements de disponibilité de l’infrastructure](#X8e3206aed4045e8fbaad84d93ea150db664eb69)
  + [8.2. Engagement de disponibilité de l’interface COMMANDITAIRE](#X86570f48e6da9370f069232b4ae175183f2dafd)
  + [8.3. Engagement de disponibilité du support](#Xfc8548982b300528a67725f1705f15805f405f0)
  + [8.4. Engagement de disponibilité du stockage objet S3](#Xd1858bb2ec86b964cb6a768cb7d9a7a780abb7b)
  + [8.5. Précision concernant l’engagement de sauvegarde](#Xcc0ee164bf81418fd2280ceac4eb569bf7b97f7)
* [9. Organisation de la relation contractuelle](#Xf5428518d06ee6569b2c74ea4a26421ab0998e2)
  + [9.1. Responsabilités du Prestataire](#X29068434a285c3f52c7ddc1ef50404d65e76fb5)
  + [9.2. Limitation des responsabilités du Prestataire](#X19121b2bd4fb4e4f45228e8bab910b62dc757c1)
  + [9.3. Limitation d’accès](#X4e70434457f7c115f116a9f6ea4ab4af9b8d941)
  + [9.4. Responsabilités des tiers participant à la fourniture du service Secure Temple](#Xc662a81cadd2baa300ca83a27240dec61621a56)
  + [9.5. Responsabilités et obligations du COMMANDITAIRE](#X53c94c34c467a68244ea6ce991e3e56c55d5d85)
  + [9.6. Droits du COMMANDITAIRE](#Xc34f07dff71165a85ac919098e14cdc0f0f59e0)
  + [9.7. Effacement des données en fin de Contrat](#X18af7e8db06fe2d84076a4e5a797e8b384bc11c)
* [10. Cycle de vie de la présente Convention de service](#X89744c1f67247955b75e73d73aaa55899645415)
  + [10.1. Entrée en effet de la Convention de service](#Xa3b4f57d1f6067d72eba0c13dc12b4e2e5a4cf1)
  + [10.2. Évolutions de la Convention de service](#Xb5b2d189dece37be8660fbd35b3e0d097bb2969)
    - [10.2.1. Évolutions déclenchées par le COMMANDITAIRE](#X946a5e541a54ab2f0ca92ca2e5ab41b3740f564)
    - [10.2.2. Évolutions déclenchées par le Prestataire](#Xe94b2234fc6249c7021ff8c044fdaa857f6a9af)
  + [10.3. Réversibilité](#X483eba08298e38537f9f27b026e82e1ece7ce7e)
* [11. Disponibilité, continuité et restauration du service](#X115fcc8f59c1201dae17a3d86136d153be01044)
  + [11.1. Gestion des Incidents et des interruptions](#X55fc305b5e53901383e26fda6b4957fbeefa9ca)
    - [11.1.1. Incidents](#X648046c564ac1cd52bebb02b256b193a3da4d74)
      * [11.1.1.1. Types d’Incidents traités dans le cadre de cette Convention de service](#X09cc1e22db275b1a463f85596829f3f871ae224)
      * [11.1.1.2. Traitement des incidents](#X726d7a25d789f16db26761d7df0c2c91f7bcc3a)
      * [11.1.1.3. Niveau de notification des Incidents de sécurité](#X61ceb4b8f57902c74fbf77bbb211197e5a82412)
  + [11.2. Maintenance du Service](#X8f50b0b400c67568e380ddb602ac786ec585905)
    - [11.2.1. Nature de la maintenance](#X903d92edf16182242ecfd404337edbaf2243b81)
    - [11.2.2. Accès distants de Cloud Temple sur le périmètre du COMMANDITAIRE](#X89ffba42dc424905d6209f36393e0e9422b9ed6)
    - [11.2.3. Accès distants de tiers participant à la fourniture du service sur le périmètre du COMMANDITAIRE](#X7ad951099cc984b8fc113222e52c4e27d11465f)
* [12. Procédure d’effacement des données en fin de Contrat](#X4ef75d4456496b7eb26b3d2dd8783cf17bd26c2)
* [13. Droit applicable](#Xdc569bbb194e0e4a197cf31537db4bf08bf3eca)
  + [13.1. De manière générale](#X5ed94d170893fb4c04d7110c419f01198fda773)
  + [13.2. Respect du droit et des réglementations applicables](#Xce704548fdd653ba3dbdfe64fefff60a0972c3f)
  + [13.3. RGPD](#Xfc35add53571984b04e4fc9d49dcfff4b7b3395)
  + [13.4. Protection vis à vis du droit extra-européen](#X5171f5ee735df20bc2100671620eddd76dca12d)
* [14. SIGNATURES](#X7ad993788a708b47017c27c9d96178e8795e44f)

# 3. Préliminaire et Glossaire

## 3.1. Préliminaire

Le présent document formalise la Convention de service associée au service IaaS qualifiée SecNumCloud sous l’appellation de « *Secure Temple*».

"La présente convention de service complète et est complémentaire aux conditions générales de vente et d’utilisation du Prestataire. Il est entendu que les documents contractuels s’interprètent de manière cohérente entre eux. En cas de contradiction ou de divergence entre les termes des documents contractuels, les documents prévaudront les uns sur les autres dans l’ordre suivant :

1. Conditions Générales de Vente et Utilisation (CGVU)
2. Convention de Service SecNumCloud IaaS
3. Convention de Service SecNumCloud PaaS
4. Convention spécifique particulière
5. Plan d’Assurance Sécurité (PAS)
6. Conditions Particulières d’Utilisation (CPU)

## 3.2. Glossaire

Dans la présente Convention de service, le **COMMANDITAIRE**, le **Prestataire** et les **Parties** sont identifiés dans le Contrat auquel est annexe la présente Convention de service.

Les expressions ci-après employées dans la présente Convention de service seront interprétées conformément aux définitions qui leur sont attribuées ci-dessous :

* **Changement :** Tout ajout, une modification ou suppression impactant le Service, ayant été autorisé, planifié ou pris en charge.
* **Changement standard :** Changement faisant l’objet d’une procédure, dont les modalités de mise en production et les impacts (y compris financiers) sont connus et acceptés à l’avance par les Parties. Il est alors intégré au catalogue des changements standards, et peut selon les cas avoir une GTI et une GTR.
* **Contrat :** désigne le contrat souscrit par le COMMANDITAIRE auprès du Prestataire pour permettre au COMMANDITAIRE de bénéficier du Service, et auquel la présente Convention de service est annexée.
* \***Convention de service :** Ce document, établi dans le cadre d’un contrat spécifique ou des Conditions Générales de Vente et d’Utilisation (CGVU), et ce, en conformité avec les exigences duRéférentiel SecNumCloud.
* **Demande de service :** demande du COMMANDITAIRE vers le Prestataire dans le cadre du Service, couvrant les opérations non réalisables par le COMMANDITAIRE depuis l’interface COMMANDITAIRE et les demandes de support dans le cadre du Service. Les demandes de service sont limitées à celles prévues au titre du Contrat ou de la présente Convention de service.
* **Disponibilité :** Capacité à assurer la disponibilité et le maintien des performances optimales du Service, en accord avec les critères et engagements définis dans les Accords de Niveau de Service (SLA).
* **Données techniques** : comprend l’ensemble des données manipulées pour délivrer le Service, notablement dont l’identité des bénéficiaires et des administrateurs de l’infrastructure technique, des journaux de l’infrastructure technique, configuration des accès, annuaire, certificats...
* **Evènement :** Un "événement" est toute occurrence détectable ou identifiable pouvant avoir une importance pour la gestion du Service.
* **Hyperviseur :** Système d’exploitation permettant l’execution de machines virtuelles sur une lame de calcul.
* **Incident :** Tout événement imprévu qui perturbe le fonctionnement normal du Service ou compromet la sécurité des données.
* **Incident de sécurité :** Tout événement dans le périmètre du Service:
  + De nature intentionnellement malveillante ;
  + De nature accidentelle portant atteinte à l’intégrité, la confidentialité ou la traçabilité du Service ou des données du COMMANDITAIRE ;
  + Portant atteinte aux mesures de sécurité existantes. Les atteintes à la Disponibilité d’origine non-malveillante ne sont pas considérées comme un Incident de sécurité (panne matérielle, bug, dysfonctionnement, sinistre naturel…).
* **Interface COMMANDITAIRE :** Interface d’administration du Service mise à disposition du COMMANDITAIRE par le Prestataire, regroupant une console d’administration web et une API.
* **Mise en production :** action(s) d’administration de réalisation du Changement quand celui-ci est approuvé (le changement, au sens ITIL, ne concernant que la gestion du changement et non sa réalisation/concrétisation).
* **Problème** : cause d’un ou plusieurs Incidents récurrents, cause d’un Incident potentiel (situation à risque).
* **Région :** désigne un ensemble géographiquement délimité de zones de disponibilité cloud, fournissant des services de réseau, de calcul et de stockage pour optimiser la latence, la performance et la conformité réglementaire locale.
* **Service :** désigne le service IaaS qualifié SecNumCloud « Secure Temple », délivré au COMMANDITAIRE par la Prestataire depuis des infrastructures techniques maintenues par le Prestataire, tel que décrit dans la section « Description du Service » de la présente Convention de service.
* **Secure Temple** : désigne le service IaaS qualifié SecNumCloud, proposé par la société Cloud Temple, tel que défini dans l’attestation consultable sur le site de l’ANSSI et fournie en annexe de la présente Convention de service.
* **Sinistre :** désigne un événement grave d’origine naturelle ou humaine, accidentelle ou intentionnelle, occasionnant des pertes et des dommages importants à la Partie sinistrée.
* **Supervision :** Surveillance d’un Système d’Information ou d’un Service, impliquant la collecte de diverses données telles que mesures et alarmes. Cette activité se limite à l’observation et au suivi, sans intervenir directement sur les éléments surveillés, une prérogative qui appartient aux opérations d’Administration.
* **Tenant :** Une instance isolée réservée à un utilisateur ou groupe d’utilisateurs, partageant une infrastructure commune tout en maintenant l’indépendance et la sécurité des données et des applications.
* **Zone de Disponibilité (AZ) (Availibility zone) :** Une section spécifique et isolée de l’infrastructure de cloud computing, conçue pour assurer la haute disponibilité et la résilience des services par une distribution géographique des ressources.

# 4. Acronymes

| **Acronyme** | **Définition** |
| --- | --- |
| **CAB** | Change Advisory Board – Comité consultatif sur les changements |
| **CMDB** | Configuration Management Database – Base de données de gestion des configurations |
| **COPIL** | Comité de pilotage |
| **COSTRAT** | Comité stratégique |
| **COPROJ** | Comité Projet |
| **DB** | Database (base de données) |
| **DRP** | Disaster Recovery Plan (PRA) (Plan de reprise d’activité) |
| **GTE** | Garantie de Temps d’Escalade |
| **GTI** | Garantie de Temps d’Intervention |
| **GTR** | Garantie de Temps de Résolution |
| **ITIL** | Information Technology Infrastructure Library - Bonnes pratiques pour la gestion des SI |
| **IaaS** | Infrastructure as a Service |
| **MCO** | Maintien en condition opérationnelle |
| **MOA** | Maitrise d’Ouvrage |
| **MOE** | Maitrise d’Œuvre |
| **MSP** | Managed Services Provider |
| **OS** | Operating system (système d’exploitation) |
| **PAQ** | Plan d’Assurance Qualité |
| **PaaS** | Platform as a Service |
| **PAS** | Plan d’Assurance Sécurité |
| **PASSI** | Prestataire d’Audit de Sécurité des Systèmes d’Information |
| **RFC** | Request For Change – Demande de changement |
| **RGPD** | Règlement Général de Protection des Données (personnelles) |
| **RPO** | Recovery Point Objective – Fraicheur des données restaurées en cas de Sinistre |
| **RTO** | Recovery Time Objective – Délai de rétablissement du service en cas de Sinistre |
| **SDM** | Service Delivery Manager |
| **SLA** | Service Level Agreement – Accord sur les niveaux de services |
| **SNC** | SecNumCloud |
| **SOC** | Security Operation Center |
| **TMA** | Tierce Maintenance dApplication |
| **UO** | Unité d’Œuvre |
| **VABE** | Validation d’Aptitude à la Bonne Exploitabilité |
| **VABF** | Validation d’Aptitude au Bon Fonctionnement |
| **VM** | Virtual Machine (Machine virtuelle) |
| **VSR** | Validation de Service Régulier |

# 5. Objet de la présente Convention de service

La présente Convention de service établit les termes et conditions selon lesquels le Prestataire s’engage à délivrer le Service au COMMANDITAIRE. Son objet est de :

* Préciser les exigences de performance attendues par le COMMANDITAIRE en termes de fonctionnalité et de fiabilité du Service ;
* Énoncer les obligations du Prestataire afin de satisfaire aux niveaux de service convenus ;
* Identifier les normes réglementaires applicables spécifiquement au Service délivré ;
* Assurer une uniformité et une intégrité dans l’évaluation de la qualité du Service ;
* Garantir l’excellence des services fournis, évaluée au moyen d’indicateurs de performance quantitatifs.

Il est stipulé que, dans l’hypothèse où le Prestataire se verrait retirer sa qualification SecNumCloud, le Contrat pourra être résilié de plein droit, sans encourir de pénalités, par le COMMANDITAIRE. Dans une telle éventualité, le Prestataire s’engage à informer le COMMANDITAIRE de cette déqualification par envoi d’une notification officielle, au moyen d’une lettre recommandée avec demande d’avis de réception.

Il convient de noter qu’une modification ou un ajustement de la qualification SecNumCloud ne sera pas interprété comme une révocation de la qualification initiale.

# 6. Audit

Le Prestataire s’engage à permettre au COMMANDITAIRE, ou à tout auditeur tiers et non concurrent du Prestataire que ce dernier aurait désigné, de consulter l’ensemble des documents nécessaires à l’attestation du respect intégral des obligations liées à la conformité avec les dispositions de l’article 28 du Règlement Général sur la Protection des Données (RGPD), facilitant ainsi la réalisation d’audits.

Par l’acceptation de la présente Convention de service, le COMMANDITAIRE confère son autorisation explicite à :

1. L’Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI) ainsi qu’à l’entité de qualification compétente pour entreprendre la vérification de la conformité du Service et de son système d’information au référentiel SecNumCloud.
2. Un prestataire d’audit de la sécurité des systèmes d’information, dûment qualifié PASSI et expressément désigné par le Prestataire, pour mener à bien des audits de sécurité portant sur le Service.

# 7. Description du Service

## 7.1. Modèle de responsabilité partagé

Le Service proposé par le Prestataire se caractérise par la mise à disposition des prestations suivantes, lesquelles s’alignent sur le principe de responsabilité partagée présenté dans le référentiel SecNumCloud :

* La provision de ressources de calcul (compute) ;
* La mise à disposition d’espaces de stockage ;
* L’accès à des services de connectivité réseau et internet ;
* L’offre d’un service de sauvegarde dédié aux machines virtuelles.

Le modèle de responsabilités partagé appliqué entre le Prestataire et le COMMANDITAIRE dans le cadre du Service est présenté en §7.1.

Il est entendu que le Prestataire mobilisera son expertise pour réaliser les Prestations selon les meilleures pratiques professionnelles et conformément aux exigences du référentiel SecNumCloud.

Le Service est qualifié SecNumCloud (voir attestation en Annexe).

## 7.2. Présentation détaillée du périmètre du Service

| Compute | Ressource de calcul du Tenant COMMANDITAIRE |
| --- | --- |
| Storage | Données de production du Tenant COMMANDITAIRE |
| Stockage objet S3 | mise à disposition d’une infrastructure de stockage objet souverain multi AZ et compatible avec les API S3 standard. |
| Sauvegarde | Modulo souscription au mass-storage adéquat |
| Infrastructure réseau | Ressource réseau du Tenant COMMANDITAIRE |
| Console COMMANDITAIRE | Le service permettant au COMMANDITAIRE d’accéder à son service IaaS et de l’administrer via l’interface Shiva |
| Support | Le service de support accompagnant les services précédents et uniquement ceux-ci (\*) |

\_(\*) Dans la limite du périmètre du Service qualifié SNC et des responsabilités du Prestataire en la matière\_

### 7.2.1. Infrastructures Datacenters

Le Service englobe la mise à disposition, pour chaque Zone de disponibilité, des prestations qualifiées ci-après :

* Site datacenter situé en France pour la Région FR, conforme aux dernières normes technologiques, avec proposant un niveau de résilience équivalent ou supérieur au niveau Tier 3 du Uptime Institute ;
* Mise à disposition de salles techniques au sein de datacenters dédiés à l’accueil des équipements techniques indispensables à la production du service, incluant calcul, stockage, réseau, câblage, et autres composants nécessaires ;
* Alimentation électrique sécurisée, assurée par deux circuits électriques distincts, garantissant une continuité de service ;
* Fourniture de services de climatisation, ajustés pour respecter les normes et préconisations des fabricants d’équipements, afin de maintenir un environnement optimal pour les dispositifs techniques ;
* Supervision continue et métrologie détaillée, permettant un suivi précis et une gestion proactive des performances et de la sécurité du service fourni.

Le Prestataire assure la mise à disposition de services avancés de détection et d’extinction d’incendie, conçus pour identifier et neutraliser efficacement tout départ de feu au sein des installations. Ces systèmes sont essentiels pour garantir la sécurité des équipements et des données. Ils comprennent des détecteurs de fumée de haute précision et des dispositifs d’extinction qui peuvent agir rapidement sans endommager l’équipement informatique. Ce service est crucial pour prévenir les risques d’incendie, minimiser les dommages potentiels et assurer la continuité des opérations.

Le COMMANDITAIRE est informé que toutes les procédures et mesures de sécurité mises en place, y compris les tests annuels de basculement sur les groupes électrogènes, sont essentielles pour garantir la continuité et l’intégrité des services fournis. Ces pratiques sont conçues pour minimiser les risques de panne et assurer une réactivité optimale en cas d’Incident. En acceptant ces conditions, le client reconnaît l’importance de ces mesures et s’engage à coopérer pleinement pour faciliter leur mise en œuvre. Le COMMANDITAIRE est également encouragé à prendre connaissance des recommandations de sécurité fournies et à les intégrer dans sa propre stratégie de gestion des risques.

### 7.2.2. Infrastructure logicielle de pilotage du Service

Le Prestataire fournit au COMMANDITAIRE la console d’administration et l’API nécessaire à l’utilisation du Service. Il s’engage également à les maintenir cette console d’administration et l’API en condition opérationnelle optimale et à en assurer la sécurité de manière continue. Cette console d’administration et l’API sont désignées de manière groupées sous le terme « interface COMMANDITAIRE ».

Le Prestataire alerte le COMMANDITAIRE sur le fait qu’une utilisation anormale de l’interface COMMANDITAIRE, notamment en cas de surcharge de ses APIs de commande (hammering), peut déclencher des mesures de sécurité automatiques entraînant le blocage de l’accès aux APIs de commande ou au Service. Il convient de souligner que cette situation ne constitue pas une indisponibilité du Service mais une action de protection du Service et de l’infrastructure du Prestataire ; par conséquent, le COMMANDITAIRE ne peut la considérer comme une indisponibilité dans ses calculs.

De plus, le Prestataire précise au COMMANDITAIRE que les requêtes parfaitement identiques (doublons) envoyées à ses APIs sont limitées à une par seconde (Throttling). Si le COMMANDITAIRE soumet des requêtes identiques à une fréquence supérieure, leur rejet ne pourra être interprété comme une indisponibilité du Service.

### 7.2.3. Infrastructures de calcul

Le Service inclut la fourniture, dans les zones de disponibilité souscrites par le COMMANDITAIRE, des équipements nécessaires à l’exécution des charges de travail sous forme de machines virtuelles.

Ceci comprend :

* La fourniture des chassis techniques nécessaires au bon fonctionnement des lames de calcul ;
* La fourniture des lames de calcul dans les quantités spécifiées par le COMMANDITAIRE et réparties selon les zones de disponibilité de son choix. Il est à noter que ces lames de calcul sont exclusivement dédiées au COMMANDITAIRE ;
* La mise à disposition de systèmes d’exploitation de type hyperviseurs, ainsi que la garantie du maintien en condition opérationnelle et de sécurité de l’infrastructure logicielle nécessaire au pilotage de ces systèmes d’exploitation. Il convient de mettre en évidence que, même si le Prestataire est responsable de la maintenance opérationnelle et de la sécurisation globale du Service, il ne détient pas de connaissances spécifiques concernant les environnements de production du COMMANDITAIRE ni des exigences liées à ses charges de travail. Par conséquent, la responsabilité de décider de la mise à jour des systèmes d’exploitation des lames de calcul hyperviseurs, une action susceptible de nécessiter un redémarrage, repose entièrement sur le COMMANDITAIRE. Cette opération peut être réalisée via l’Interface COMMANDITAIRE.

Le choix du modèle de lame de calcul, sélectionné parmi le catalogue proposé par le Prestataire, relève de la responsabilité du COMMANDITAIRE.

### 7.2.4. Infrastructure de stockage

Le service comprend la fourniture au COMMANDITAIRE d’une infrastructure de stockage partagée de type SAN (Storage Area Network), offrant divers niveaux de performance. Ce service englobe :

* L’implémentation et le maintien en condition opérationnelle et en condition de sécurité du réseau SAN dédié ;
* L’installation et la gestion des baies de stockage mutualisées entre les clients, y compris leur maintien en condition opérationnelle et en condition de sécurité, leur supervision et leur métrologie ;
* La mise en place des systèmes automatisés pour l’allocation des LUNs (Logical Unit Numbers) de stockage dédiés à l’usage du COMMANDITAIRE, conformément aux volumes souscrits par le COMMANDITAIRE.

### 7.2.5. Infrastructure réseau globale

Le Prestataire déploie dans le cadre du Service, un réseau global facilitant au COMMANDITAIRE la mise en accessibilité de ses systèmes hébergés. Ce service comprend :

* La fourniture, le maintien en condition opérationnelle et en condition de sécurité de l’ensemble des liaisons en fibres optiques interconnectant les différentes Zones de disponibilité;
* La fourniture, le maintien en condition opérationnelle et en condition de sécurité des équipements techniques nécessaires au bon fonctionnement du réseau et à l’isolation des différents clients.

L’interconnexion réseau du Tenant COMMANDITAIRE, à Internet ou à des réseaux privés, et les équipements réseaux, liens opérateurs et autres composants techniques réalisant cette interconnexion, ne font pas partie du périmètre du Service. Cette interconnexion réseau est mise en œuvre conformément aux dispositions prévues dans le Contrat.

### 7.2.6. Infrastructure de sauvegarde

Le Prestataire met à disposition du COMMANDITAIRE un service de sauvegarde intégré, dédié et géré, destiné à la protection de ses machines virtuelles. Le Prestataire assure le maintien en condition opérationnelle et en condition de sécurité de ce service de sauvegarde. Le Prestataire garantit que les sauvegardes du COMMANDITAIRE seront situées en dehors de la Zone de disponibilité des charges de travail sauvegardées, sous réserve que le COMMANDITAIRE ait souscrit au Unités d’œuvre adéquates.

Cette prestation de sauvegarde se limite à la sauvegarde des machines virtuelles et des configurations de topologie de l’environnement IaaS des Tenants du COMMANDITAIRE dans le cadre du Service. L’élaboration et l’application d’une politique de sauvegarde adéquate par le COMMANDITAIRE dépendent de la souscription à des unités d’œuvre spécifiques. Il incombe donc au COMMANDITAIRE de s’assurer de la disponibilité des ressources techniques nécessaires auprès du Prestataire pour mettre en œuvre sa politique de sauvegarde ou d’ajuster cette dernière en fonction des moyens disponibles.

Le Prestataire s’engage à notifier le COMMANDITAIRE en cas de contraintes de capacité et à fournir une assistance conseil pour l’optimisation des ressources. Les obligations du Prestataire se limiteront à la mise en œuvre des besoins exprimés par le COMMANDITAIRE en matière de politique de sauvegarde, dans le cadre des ressources souscrites.

### 7.2.7. Mise en œuvre de solutions de reprise d’activité ou de continuité d’activité

Le Prestataire fournit au COMMANDITAIRE l’ensemble des solutions techniques nécessaires pour garantir une répartition optimale de ses ressources à travers diverses Zones de disponibilité. Il incombe au COMMANDITAIRE la responsabilité de gérer efficacement cette distribution de ressources, pour laquelle il a la possibilité à exploiter les outils du Prestataire disponibles à cet usage.

## 7.3. Limitations des services dans le modèle IaaS qualifié

### 7.3.1. Services managés en RUN

Il est important de noter que sont écartés du Service :

* L’hébergement de composants physiques du COMMANDITAIRE ;
* L’interconnexion réseau du Tenant COMMANDITAIRE, à Internet ou à des réseaux privés, incluant les liens opérateur ;
* Tout service de type managé, ou TMA;
* Toute assistance sur les machines virtuelles au niveau OS et au-dessus dans la pile de responsabilités Iaa, même s’il s’agit de simple supervision.

Cela étant, il n’est absolument pas exclu que le COMMANDITAIRE ait recours à de tels services auprès de l’offre MSP du Prestataire pour intervenir en mode services managés sur ses Tenants. Ces services ne seront alors pas encadrés par la présente Convention de service et ses engagements/clauses bipartites.

### 7.3.2. Configuration du secours

Par défaut, le Prestataire fournit la mise en place des ressources du IaaS au COMMANDITAIRE en réservant des ressources et en configurant les déploiements pour utiliser les Zones de disponibilité. Il incombe au COMMANDITAIRE de choisir les Zones de disponibilité via l’interface COMMANDITAIRE.

### 7.3.3. Configuration de la sauvegarde

La prestation de sauvegarde s’arrête à la sauvegarde des machines virtuelles et des configurations de topologie représentant l’environnement IaaS des Tenants du COMMANDITAIRE dans le cadre du Service.

La prestation de sauvegarde et la complétion de la politique de sauvegarde du COMMANDITAIRE est soumise à la souscription d’espace de stockage sur le mass storage nécessaire pour assurer le service. Il est donc de la responsabilité du COMMANDITAIRE de souscrire auprès du Prestataire les moyens techniques nécessaires pour assurer la politique de sauvegarde sur son périmètre informatique, ou d’ajuster la politique de sauvegarde aux moyens mis en œuvre. Le Prestataire s’engage à informer le COMMANDITAIRE en cas de limite de capacité technique.

Le Prestataire mettra en place les moyens techniques et humains nécessaires à la sauvegarde du système hébergé dans la limite des ressources souscrites par le COMMANDITAIRE.

Par ailleurs, dans le cas des périmètres non pris en charge par le Prestataire, il appartient au COMMANDITAIRE de définir sa propre stratégie de sauvegarde et de paramétrer lui-même les sauvegardes des VM ou d’effectuer une Demande de service auprès du Prestataire pour que le paramétrage des sauvegardes pour les serveurs physiques soit mis en place si le COMMANDITAIRE dispose d’un contrat de service managé permettant au Prestataire d’agir via l’interface COMMANDITAIRE qui est la console d’administration qui est mise à disposition dans le cadre de cette Convention de service et qui dispose de fonctionnalités pour configurer les sauvegardes.

En outre, ce service n’aura comme engagement que de traduire par le paramétrage via l’interface COMMANDITAIRE, la configuration spécifiée clairement par le COMMANDITAIRE.

Pour des raisons de flexibilité de l’offre du Prestataire, le COMMANDITAIRE a l’option d’associer une politique de non-sauvegarde sur certaines de ses VM. Dans ce cas, il appartient au COMMANDITAIRE d’assumer ce choix. Le Prestataire ne sauvegardera pas les VM associées à la politique "no backup". Le Prestataire alerte le COMMANDITAIRE que choisir la politique "no backup" ou choisir de sauvegarder manuellement expose le COMMANDITAIRE à une perte de données définitive en cas d’Incident sur les couches basse ou sur les couches dépendant de sa responsabilité dans le modèle IaaS. Dans un tel cas, il sera impossible de tenir le Prestataire responsable de restaurer les données car il n’y aura rien à restaurer. Le Prestataire recommande de toujours sauvegarder les VM.

Pour tout sujet concernant l’OS installé sur une machine virtuelle et tout logiciel ou programme exécuté « par-dessus l’OS », il est de la responsabilité du COMMANDITAIRE de réaliser les opérations d’administration et de supervision au sein de l’Union Européenne s’il souhaite garantir que toute la verticalité des couches du SI soient opérées et gérées depuis l’Union Européenne. Les opérations d’administration hors du périmètre de responsabilité du Prestataire dans le cadre de la présente Convention de service dont indiquées dans la section « Modèle de responsabilités partagées » de la présente Conventions de Service.

## 7.4. Mise en œuvre du service

### 7.4.1. Prérequis techniques

Pour la mise en œuvre du Service, le COMMANDITAIRE reconnaît qu’il devra :

* Fonctionner avec une virtualisation de type VMware dans les versions supportées par l’éditeur et fournies par le Prestataire dans le cadre du Service;
* Recourir via le Prestataire à l’utilisation de l’outil de sauvegarde;
* Déclarer des IP fixes depuis lesquelles le Prestataire l’autorisera à accéder à l’interface COMMANDITAIRE (Filtrage par liste blanche). Les modifications de cette liste d’IP devront être réalisées via des Demandes de service (liste non administrable depuis l’interface d’administration du Service).

## 7.5. Localisation du service en France

Il est précisé qu’aucune des opérations et aucun des composants physiques impliqués dans la fourniture du Service , dont la présente Convention de service fait l’objet, n’est situé hors de l’Union Européenne.

Cela inclut notamment le support, la supervision opérationnelle et la supervision de sécurité (SOC) de l’infrastructure technique délivrant le Service. De fait, tout le stockage, toutes les tâches d’administration, de supervision et tous les traitements sont réalisés en France.

### 7.5.1. Localisation des Datacenters hébergeant le Service

A défaut des opérations des collaborateurs et des agences du Prestataire, l’ensemble des opérations de production (comprenant le stockage et le traitement des données) et composants techniques délivrant le Service sont situés dans les Datacenters basés en France.

### 7.5.2. Localisation des agences Cloud Temple opérant le service

Les collaborateurs de Cloud Temple intervenant sur le périmètre duService opèrent depuis les agences de Cloud Temple toutes situées exclusivement en France. Ces agences sont situées en France, à Tours, Lyon, Caen et Paris La Défense.

Le COMMANDITAIRE est informé de la possibilité des salariés de Cloud Temple de travailler à distance. Toutefois, le Prestataire garantit le même niveau de sécurité concernant les accès à distance, notamment concernant les accès VPN. Ces accès distants sont mis en œuvre conformément aux exigences du référentiel SecNumCloud.

## 7.6. Support

### 7.6.1. Nature du support accompagnant le service

Le Prestataire fournit un service de support technique visant à assister le COMMANDITAIRE dans la gestion, le dépannage et l’optimisation de leurs ressources déployées. Ce service couvre une gamme étendue d’activités, depuis l’aide à la configuration initiale des services jusqu’au soutien technique avancé pour résoudre des problèmes spécifiques.

Voici une description des caractéristiques et fonctionnalités du service de support :

* Assistance à la mise en œuvre initiale de l’utilisation du Service ;
* Assistance à la résolution d’incidents ;
* Assistance à la résolution de problèmes ;
* Suivi et conseil sur l’optimisation du socle technique.

Dans le cadre du service de support, le Prestataire ne se substitue pas au COMMANDITAIRE dans l’usage du Service. Le COMMANDITAIRE reste entièrement responsable de la configuration, de l’exploitation de ses VM et de ses Tenants, et de la gestion de tous les éléments (données et applications incluses) qu’il a stockés ou installés sur les infrastructures du Prestataire. Le service de support technique est fourni en accord avec les Conditions Générales de Vente et d’Utilisation, le Prestataire étant tenu à une obligation de moyens.

Le COMMANDITAIRE s’engage à utiliser le service de support technique de manière raisonnable, s’abstenant notamment de solliciter des services non souscrits auprès du Prestataire et de faire intervenir les équipes du Prestataire auprès de ses propres clients ou de tiers non inclus dans le Contrat. Le Prestataire se réserve le droit de rejeter toute demande de service ne respectant pas ces critères.

Le niveau d’engagement du support est conditionné à la souscription des unités d’œuvre de support associées.

### 7.6.2. Sollicitation du service support technique

Le support technique est accessible par le biais d’un système de tickets via la console COMMANDITAIRE et est disponible durant les heures normales de bureau hors jours fériés (8h - 18h ; Lundi – Vendredi ; calendrier et horaires français). Pour les urgences survenant en dehors des heures ouvrées, notamment les incidents affectant significativement la production, le service d’astreinte peut être joint via un numéro communiqué au COMMANDITAIRE à l’initialisation du Service.

Pour chaque demande ou Incident, il est impératif de générer un ticket auprès du support du Prestataire. L’initialisation de ce ticket, comprenant toutes les informations nécessaires, est essentielle et marque le début de l’évaluation des engagements du Prestataire.

Dès que le Prestataire reçoit une demande ou une notification d’Incident, que ce soit par le biais de la console de gestion ou à la suite d’un appel téléphonique, un ticket est automatiquement créé. Lors de la déclaration d’un Incident, il est essentiel que le COMMANDITAIRE fournisse au prestataire un maximum de détails sur le problème rencontré. Cette démarche est cruciale pour permettre une évaluation adéquate de la situation, sa priorisation et un diagnostic efficace.

Le Client reçoit alors une confirmation par courriel, indiquant la création du ticket et son numéro unique. Le COMMANDITAIRE peut consulter le statut et l’historique de ses demandes et déclarations d’Incidents directement depuis la console de gestion.

### 7.6.3. Processus de gestion des Incidents

Lors d’une déclaration d’un Incident, l’équipe de support technique du Prestataire initie une investigation pour identifier la cause du problème et établir un diagnostic. Le Client doit collaborer activement avec le Prestataire en fournissant toutes les informations nécessaires et en effectuant les tests requis. Le Prestataire peut accéder au Service du Client pour diagnostiquer l’Incident.

Si les Services du Prestataire sont jugés fonctionnels et que l’Incident ne lui est pas imputable, le Client en sera informé. À la demande du Client, le Prestataire peut proposer des Services Professionnels pour identifier l’origine du problème, facturable sur accord préalable par tranche de 30mn.

Dans le cas où l’Incident est de la responsabilité du Prestataire ou de l’un de ses sous-traitants, celui-ci complète le diagnostic et s’attèle à la restauration du Service sans frais supplémentaires. Le diagnostic s’appuie sur les échanges entre les Parties et les données du Prestataire, ces éléments étant considérés comme probants par accord des Parties.

### 7.6.4. Processus de priorisation des traitements

La détermination du niveau de priorité d’un dossier repose sur une analyse matricielle qui évalue l’impact de l’Incident et son degré de criticité :

* Les niveaux d’impact sont définis de la manière suivante :

| Niveau d’impact | Description |
| --- | --- |
| Impact I1 | Le ou les services du Prestataire sont interrompus |
| Impact I2 | Le ou les services du Prestataire sont dégradés |
| Impact I3 | Le ou les services du Prestataire sont actuellement stable, mais montrent des signes de potentiel déclin à long terme |

* Les niveaux de Criticités sont définis de la manière suivante :

| Niveau de criticité | Description |
| --- | --- |
| Criticité C1 | Le ou les services du Prestataire se dégradent à une vitesse préoccupante |
| Criticité C2 | Le ou les services du Prestataire se détériore progressivement au fil du temps |
| Criticité C3 | Le ou les services du Prestataire présentes un ou plusieurs inconvenient sans conséquence significative |

* Sur la base d’une analyse approfondie de la situation, prenant en compte les éléments déterminant l’Impact et la Criticité, une priorité est attribuée au ticket conformément à la matrice de décision ci-après :

| Niveau d’impact  Niveau de criticité | Impact I1 | Impact I2 | Impact I3 |
| --- | --- | --- | --- |
| Criticité C1 | Priorité **P1** | Priorité **P2** | Priorité **P3** |
| Criticité C2 | Priorité **P2** | Priorité **P3** | Priorité **P4** |
| Criticité C3 | Priorité **P3** | Priorité **P4** | Priorité **P5** |

Les engagements de niveau de service correspondant à chaque niveau de priorité sont détaillés dans le chapitre suivant.

### 7.6.5. Langue et localisation du service de support

Le support est fourni par le Prestataire au COMMANDITAIRE a minima en langue française. Le support peut être également fourni en langue anglaise.

Les opérations du service de support du Prestataire pour l’offre de service d’infrastructure qualifiée SecNumCloud sont situées dans l’Union Européenne.

# 8. Engagements et niveaux de services

Le Prestataire s’engage à garantir une surveillance continue de la performance et de l’intégrité sécuritaire de son infrastructure technique délivrant le Service, veillant à leur fonctionnement optimal.

L’indisponibilité d’un service, faisant l’objet d’un indicateur de performance, est reconnue dès son identification par le système de supervision du Prestataire, ou suite à une notification par un utilisateur du COMMANDITAIRE. Le début de l’indisponibilité est fixé au moment le plus précoce entre ces deux événements, afin de garantir un décompte précis et juste du temps d’indisponibilité.

La fin de l’indisponibilité est officiellement marquée par la restauration complète du service, confirmée soit par les outils de supervision du Prestataire, soit par un retour utilisateur, assurant ainsi une reprise effective des opérations et une mesure fidèle de la durée de l’interruption.

## 8.1. Engagements de disponibilité de l’infrastructure

Le Prestataire s’engage à maintenir un niveau de disponibilité et de performance conforme aux standards définis pour chaque période spécifiée. Les engagements de niveau de service (Service Level Agreements, SLAs) s’appliquent sous réserve que le COMMANDITAIRE implémente ses systèmes à travers au moins deux des Zones de disponibilité présentes dans la Région concernée.

En l’absence de respect de ces conditions par le COMMANDITAIRE, celui-ci se verra dans l’incapacité de revendiquer l’application des SLAs concernés, lesquels sont spécifiquement identifiés par un astérisque (\*). L’accessibilité aux SLAs se fait via l’interface COMMANDITAIRE. Les mesures s’entendent calculées mensuellement :

* \*\*SLA 1 (\*) : IC-INFRA\_SNC-01\*\* – Disponibilité de la puissance de calcul (Compute) : taux de disponibilité garanti de 99,99%, calculé sur une base 24h/24, 7j/7.
* \*\*SLA 2 (\*) : IC-INFRA\_SNC-02\*\* – Disponibilité du stockage : taux de disponibilité garanti de 99,99%, calculé sur une base 24h/24, 7j/7.
* **SLA 3 : IC-INFRA\_SNC-03** – Fiabilité de la sauvegarde : taux de disponibilité garanti de 99,99%, calculé sur une base 24h/24, 7j/7.
* \*\*SLA 4 (\*) : IC-INFRA\_SNC-04\*\* – Disponibilité de l’infrastructure réseau : taux de disponibilité garanti de 99,99%, calculé sur une base 24h/24, 7j/7.
* **SLA 5 : IC-INFRA\_SNC-05** – Accès Internet : taux de disponibilité garanti de 99,99%, calculé sur une base 24h/24, 7j/7.

***Remarques*** :

* *En réponse une attaque par déni de service distribué (DDoS), le Prestataire se réserve le droit d’ajuster sa configuration de routage internet pour limiter l’impact de cette attaque et sauvegarder son infrastructure. En particulier, si une adresse IP appartenant au COMMANDITAIRE est ciblée, le Prestataire peut recourir à la technique de blackholing via la communauté BGP pour bloquer tout le trafic vers l’adresse IP visée en amont chez ses fournisseurs, dans le but de protéger les ressources du COMMANDITAIRE ainsi que celles d’autres COMMANDITAIREs et de l’infrastructure du Prestataire. Le Prestataire encourage vivement le COMMANDITAIRE à adopter des mesures similaires, telles que l’utilisation de logiciels de pare-feu d’applications web disponibles sur le marché, et à configurer soigneusement ses groupes de sécurité via l’API de commande.*
* *Le Prestataire insiste sur la nécessité pour le COMMANDITAIRE de minimiser les ouvertures de flux, en évitant notamment de rendre accessibles les ports d’administration* ***SSH*** *(port TCP 22) et* ***RDP*** *(port TCP 3389) depuis l’ensemble d’Internet (sous-réseau 0.0.0.0/0), ainsi que les protocoles internes tels que* ***SMB*** *(port TCP/UDP 445) ou* ***NFS*** *(port TCP/UDP 2049).*

## 8.2. Engagement de disponibilité de l’interface COMMANDITAIRE

* SLA 6 : IC-INFRA\_SNC-06 – Accès à la console d’administration du Service : une disponibilité garantie de 97%, assurée en continu, 24 heures sur 24 et 7 jours sur 7.
* SLA 7 : IC-INFRA\_SNC-07 – Accès aux APIs de pilotage du Service : une disponibilité de 99.9%, calculé sur une base 24h/24, 7j/7.

## 8.3. Engagement de disponibilité du support

* **SLA 8 : IC-INFRA\_SNC-08** – Voici les engagements de performance du support technique du Prestataire pour les incidents, hors maintenances programmées :

| Priorité | Garantie de temps d’intervention (GTI) | Objectif de performance |
| --- | --- | --- |
| Priorité **P1** | 30mn | 95% |
| Priorité **P2** | 2h | 90% |
| Priorité **P3** | 4h | 90% |
| Priorité **P4** | 24h | 85% |
| Priorité **P5** | 48h | 85% |

* **SLA 9 : IC-INFRA\_SNC-09** – Voici les engagements de performance du support technique du Prestataire pour les demandes de service :

|  | Garantie de temps d’intervention (GTI) | Objectif de performance |
| --- | --- | --- |
| Demande de service | 4h | 90% |

*Nota* :

* *Le délai pour la Garantie de Temps d’Intervention (GTI) est calculé à partir de la différence entre le moment où le COMMANDITAIRE ouvre le ticket et la première intervention du support du Prestataire.*
* *L’investigation d’incidents concernant les COMMANDITAIREs ne comprendra pas d’intervention à distance sur les serveurs hébergés du COMMANDITAIRE. Cette assistance se limitera à l’explication des métriques disponibles relatives à l’environnement du COMMANDITAIRE, afin de faciliter la compréhension des incidents ou des problèmes de performance rencontrés. Sur la base des résultats de cette analyse, des recommandations pourront être suggérées.*

## 8.4. Engagement de disponibilité du stockage objet S3

* **SLA 10 : IC-INFRA\_SNC-10** – Voici les engagements de disponibilité pour le stockage objet S3 :

| Indicateur | Engagement | Objectif de disponibilité |
| --- | --- | --- |
| IC-INFRA-SNC-10.1 | Durabilité du stockage d’un objet sur une région | 99.9999999% / an |
| IC-INFRA-SNC-10.2 | Disponibilité de l’API Stockage Objet S3 | 99.99% |
| IC-INFRA-SNC-10.3 | Latence maximale d’accès à un objet sur une région | 150 ms |

Remarques :

* Le Service de Stockage Objet est spécifiquement conçu pour le stockage d’objets et doit être employé dans ce seul but, **excluant catégoriquement son utilisation en mode bloc**. Recourir au mode bloc par des méthodes détournées, incluant par exemple l’utilisation de *“FUSE” dans un environnement Linux*, constitue une infraction aux termes d’utilisation énoncés. Aucun incident, dysfonctionnement ou dommage découlant de cet usage non conforme ne sera couvert par les Accords de Niveau de Service (SLA) définis dans cette convention de services.
* La garantie de durabilité est conditionnée à une utilisation des services conforme aux meilleures pratiques et standards actuels, et exclut explicitement toute modification des données, qu’elle soit intentionnelle ou accidentelle, résultant d’actions entreprises par le COMMANDITAIRE.

## 8.5. Précision concernant l’engagement de sauvegarde

La stratégie de sauvegarde déployée pour le COMMANDITAIRE, est conditionnée par la souscription aux unités d’œuvre adéquates.

Le Prestataire s’engage sur la mise à disposition d’une solution de sauvegarde qui permettra au COMMANDITAIRE d’appliquer les politiques de sauvegardes souhaitées.

Il est précisé que le périmètre du Prestataire s’arrête à la mise à disposition d’un service de sauvegarde et c’est au COMMANDITAIRE de superviser via l’interface COMMANDITAIRE la bonne exécution des politiques associées.

Il est précisé que la gestion de capacités de stockage de l’espace de stockage dédié aux sauvegardes, reste à la charge et responsabilité du COMMANDITAIRE. Le Prestataire met à disposition le taux d’utilisation via la console.

*Exemple : Non sauvegarde d’une machine virtuelle :*

*Le COMMANDITAIRE a la charge de vérifier / superviser la bonne exécution des politiques des sauvegardes, dans le cas où le COMMANDITAIRE constate qu’une machine virtuelle n’est pas sauvegardée, il lui appartient d’en vérifier la cause, le COMMANDITAIRE pourra solliciter le Support du Prestaire selon le niveau de support souscrit pour être assisté.*

**Le SLA 8 : IC-INFRA\_SNC-08 et SLA 9**, sera exclusivement applicable dans le cas d’un Incident du service sauvegarde.

# 9. Organisation de la relation contractuelle

## 9.1. Responsabilités du Prestataire

Le Prestataire s’engage :

* à informer son COMMANDITAIRE de manière adéquate (par exemple en cas de limite de capacité de ressources techniques délivrant le Service).
* à informer formellement le COMMANDITAIRE et dans un délai d’un mois, de tout​ changement juridique, organisationnel ou technique pouvant avoir un impact sur la conformité du Service aux exigences de protection contre les lois extra-européennes (19.6 du référentiel SNC v3.2).
* à fournir au COMMANDITAIRE des interfaces et des interfaces de service qui sont en langue française a minima.
* à étudier et prendre en compte les exigences sectorielles spécifiques liées aux types d’informations confiées par le COMMANDITAIRE dans le cadre de la mise en œuvre du service et dans la limite des responsabilités du Prestataire.
* à ne divulguer aucune information relative à la prestation à des tiers, sauf autorisation formelle et écrite du COMMANDITAIRE.
* à mettre à disposition toutes les informations nécessaires à la réalisation d’audits de conformité conformément aux dispositions de l’article 28 du RGPD.
* à rendre compte auprès du COMMANDITAIRE, par la présente Convention de service, de tout Incident de sécurité impactant le Service ou l’utilisation faite par le COMMANDITAIRE du Service (incluant les données du COMMANDITAIRE).
* à autoriser un prestataire d’audit de la sécurité des systèmes d’information (PASSI) qualifié, mandaté par le Prestataire, à auditer le service ainsi que son système d’information, conformément au plan de contrôle du SecNumCloud du Prestataire. De plus, le Prestataire s’engage à fournir toutes les informations nécessaires pour mener à bien les audits de conformité aux dispositions de l’article 28 du RGPD, menés par le commanditaire ou un tiers mandaté.
* à fournir, en qualité de sous-traitant, conformément à l’article 28 du Règlement général sur la protection des données (RGPD), assistance et conseils au COMMANDITAIRE en l’alertant dès lors qu’une instruction émise par ce dernier est susceptible de constituer une violation des règles de protection des données.
* à notifier par écrit, lorsqu’un projet impacte ou est susceptible d’impacter le niveau de sécurité du Service, le COMMANDITAIRE des potentiels impacts, des mesures d’atténuation mises en place, ainsi que des risques résiduels qui le concernent.
* à documenter et à mettre en œuvre l’ensemble des procédures nécessaires pour respecter les exigences légales, réglementaires et contractuelles applicables au service, ainsi que les besoins de sécurité spécifiques du COMMANDITAIRE, définis par ce dernier et prévus au Contrat. Sur demande du COMMANDITAIRE, le module Documentation de l’interface COMMANDITAIRE permettra un partage sécurisé de ces documents.
* à fournir, sur demande du COMMANDITAIRE, les éléments d’appréciation des risques relatifs à la soumission des données du COMMANDITAIRE au droit d’un état non-membre de l’Union Européenne.

Sur demande du COMMANDITAIRE formelle et écrite, le Prestataire s’engage à :

1. Rendre accessible au COMMANDITAIRE le règlement intérieur et la charte d’éthique du Prestataire ;
2. Rendre accessible au COMMANDITAIRE les sanctions encourues en cas d’infraction à la politique de sécurité ;
3. Fournir au COMMANDITAIRE l’ensemble des événements le concernant dans les éléments de journalisation du Service ;
4. A la fin du Contrat le Prestataire s’engage à supprimer les données et Données techniques relatives au COMMANDITAIRE, conformément à la « procédure d’effacement des données en fin de Contrat » décrite dans la présente Convention de service.
5. à assurer un effacement sécurisé de l’intégralité des données du COMMANDITAIRE par réécriture complète de tout support ayant hébergé ses données dans le cadre du Service.
6. à fournir la liste complète des tiers autorisés à accéder aux infrastructures portant les données.

Le Prestataire maintiendra à jour et mettra à disposition du COMMANDITAIRE la liste exhaustive des tiers autorisés à accéder aux infrastructures portant les données, informant ce dernier de tout changement relatif aux sous-traitants. Le Prestataire et l’ensemble de ses filiales s’engagent à respecter les valeurs fondamentales de l’Union européenne, à savoir la dignité humaine, la liberté, la démocratie, l’égalité, l’état de droit, ainsi que le respect des Droits de l’homme. Le service fourni par le Prestataire est conforme à la législation en vigueur en matière de droits fondamentaux et aux valeurs de l’Union européenne relatives au respect de la dignité humaine, à la liberté, à l’égalité, à la démocratie et à l’État de droit.

## 9.2. Limitation des responsabilités du Prestataire

Du fait de l’ensemble des définitions et conditions mentionnées dans la présente Convention de service, les responsabilités du Prestataire sont limitées ainsi :

1. Le modèle de responsabilité partagée, décrit dans la section « Modèle de responsabilités partagées » de la présente Convention de service, limite de fait l’implication du Prestataire dans les couches de fonctionnement allant “au-dessus” de la mise à disposition de ressources de calcul, de réseau, de stockage et de sauvegarde. Ceci exclut en particulier sans s’y limiter :
   * La gestion de ce qui est installé sur les machines virtuelles (OS, middlewares, applicatifs, etc.);
   * La tenue à jour des OS et autres logiciels installés par le COMMANDITAIRE sur ses machines dans ses Tenants;
   * La sécurité des programmes, logiciels et applicatifs installés sur les machines virtuelles;
   * La mise à jour des machines virtuelles;
   * La sauvegarde des données au niveau applicatif.
2. Le Prestataire ne peut prendre d’engagements de sauvegarde des Tenants du COMMANDITAIRE sans que le COMMANDITAIRE n’ai au préalable souscrit aux unités d’oeuvres adéquates.
3. Le Prestataire ne peut se prévaloir de la propriété des données transmises et générées par le COMMANDITAIRE. En effet, celles-ci relèvent de la propriété du COMMANDITAIRE.
4. Le Prestataire souligne qu’il ne peut en aucun cas exploiter les données transmises et générées par le COMMANDITAIRE sans validation préalable de ce dernier.
5. Le Prestataire dégage toute responsabilité sur les composants physiquement hébergés et infogéré par le Prestataire, mais étant la propriété directe du COMMANDITAIRE ou d’un tiers avec lequel le COMMANDITAIRE a contractualisé. L’hébergement de composants physiques des clients ne fait pas partie du Service et est de fait hors du cadre de la présente Convention de service. Il incombe au COMMANDITAIRE d’évaluer le niveau d’adhérence ou de dépendance qu’introduisent ces composants vis-à-vis du Service IaaS qualifié SecNumCloud.

## 9.3. Limitation d’accès

Dans le cadre du Service, le Prestataire est formellement interdit d’accéder aux Tenants appartenant au COMMANDITAIRE sans autorisation préalable. Il est de la responsabilité du COMMANDITAIRE de fournir les accès nécessaires au personnel du Prestataire, selon les besoins spécifiques de l’hébergement et, le cas échéant, des services professionnels de support, si cette option a été choisie par le COMMANDITAIRE.

Le COMMANDITAIRE reconnaît que ces accès sont accordés exclusivement pour les besoins liés à la prestation de services convenus, assurant ainsi une gestion sécurisée et conforme aux termes de l’accord.

L’accès distant par des tiers impliqués dans la prestation de service du Prestataire est strictement interdit. Dans l’éventualité où une exigence technique spécifique nécessiterait un tel accès, celui-ci ne pourrait être établi qu’après avoir clairement notifié le COMMANDITAIRE, fourni une justification détaillée et obtenu son accord écrit.

Cette mesure garantit le contrôle et la sécurité des données du COMMANDITAIRE, en s’assurant que toute exception à la règle est dûment autorisée et documentée.

## 9.4. Responsabilités des tiers participant à la fourniture du service Secure Temple

Le Prestataire maîtrise la liste des tiers partenaires participant de la fourniture du Service. Ces tiers sont les éditeurs, prestataires (du Prestataire) et autres fournisseurs participant de la fourniture du Service. Le Prestataire applique les mesures suivantes à ces tiers :

* Le Prestataire exige des tiers participant à la mise en œuvre du service, dans leur contribution au Service, un niveau de sécurité au moins équivalent à celui qu’il s’engage à maintenir dans sa propre politique de sécurité applicable au service Secure Temple ;
* Le Prestataire contractualise, avec chacun des tiers participant à la mise en œuvre du service, des clauses d’audit permettant à un organisme de qualification de vérifier que ces tiers respectent les exigences légales et les exigences SNC, permettant au Prestataire de respecter ses engagements dans la présente Convention de service.
* Le Prestataire met en œuvre une procédure permettant de contrôler régulièrement les mesures mises en place par les tiers participant à la mise en œuvre du service pour respecter les exigences au Prestataire de respecter ses engagements dans la présente Convention de service.
* Le Prestataire met en œuvre une procédure de suivi des changements apportés par les tiers participant à la mise en œuvre du service susceptibles d’affecter le niveau de sécurité du système d’information du service.

## 9.5. Responsabilités et obligations du COMMANDITAIRE

Pour rappel, le Prestataire fournit au COMMANDITAIRE une plateforme d’execution de machines virtuelles, la configuration de celles-ci est à la charge du COMMANDITAIRE. Chaque machine virtuelle ne peut fonctionner sans une politique de sauvegarde associée. Le Prestataire définit via ses interfaces des politiques de sauvegarde automatiques. Mais c’est à la charge du COMMANDITAIRE l’activation de ces politiques de sauvegarde et donc d’activer les machines virtuelles.

Le COMMANDITAIRE autorise l’ANSSI et l’organisme de qualification SNC à auditer le Service et l’infrastructure technique délivrant le Service.

## 9.6. Droits du COMMANDITAIRE

À tout moment au cours de la relation contractuelle, le COMMANDITAIRE peut déposer une réclamation relative au service qualifié auprès de l’ANSSI.

À tout moment, le COMMANDITAIRE peut demander au Prestataire de lui rendre accessible son règlement intérieur et sa charte d’éthique.

## 9.7. Effacement des données en fin de Contrat

À l’issue du contrat, qu’il arrive à échéance ou qu’il soit résilié pour quelque raison que ce soit, le Prestataire s’engage à procéder à l’effacement sécurisé de l’intégralité des données du COMMANDITAIRE, y compris les données techniques. Le Prestataire s’assurera de communiquer au COMMANDITAIRE un préavis formel, respectant un délai de vingt et un (21) jours calendaires. Les données du COMMANDITAIRE seront alors supprimées dans un délai maximum de trente (30) jours suivant cette notification.

Pour attester de cette suppression, le Prestataire remettra au COMMANDITAIRE un certificat confirmant l’effacement des données.

# 10. Cycle de vie de la présente Convention de service

## 10.1. Entrée en effet de la Convention de service

La présente Convention de service entre en effet le jour de sa signature par le COMMANDITAIRE.

La collecte, la manipulation, le stockage et le traitement des données faits dans le cadre de l’avant-vente, la mise en œuvre, l’arrêt du Service​, sont faits dans le respect de la législation en vigueur.

## 10.2. Évolutions de la Convention de service

Les modifications ou ajouts apportés à la présente Convention de service découlent exclusivement des requêtes formulées par les organes de gouvernance désignés à cet effet. Ces propositions de changement seront examinées par les Parties, habilitées à déterminer les aspects nécessitant une formalisation écrite.

Il est convenu que toute évolution de la Convention de service, après validation, qui altère les conditions financières initialement établies, nécessitera l’établissement et la signature d’un avenant au Contrat en cours.

Les facteurs pouvant induire une révision de cette Convention de service incluent, sans s’y limiter :

* L’évolution de l’infrastructure technique délivrant le Service IaaS ;
* Les ajustements apportés aux services déployés par le Prestataire pour fournir le Service ;
* Les variations des engagements pris et des sanctions applicables ;
* Les reconfigurations organisationnelles au sein du COMMANDITAIRE ou du Prestataire ;
* L’expansion ou la réduction du champ d’application du Service.

La gestion des versions et des révisions de la Convention de service est consignée en préambule du document pour en faciliter le suivi.

### 10.2.1. Évolutions déclenchées par le COMMANDITAIRE

Les évolutions de la Convention de service peuvent avoir, notamment, pour origine :

* Une évolution de l’infrastructure gérée par le Prestataire ;
* Une modification des services mis en œuvre par le Prestataire ;
* Une modification des engagements de niveaux de services par le Prestataire.

### 10.2.2. Évolutions déclenchées par le Prestataire

Toute modification de la Convention de service est soumise à acceptation du COMMANDITAIRE. Il est entendu que toute modification ou complément validés modifiant les éléments financiers du Contrat, pourra impliquer la signature d’un avenant à celui-ci.

## 10.3. Réversibilité

De plus, Cloud Temple s’engage à permettre une révision de la présente Convention de service (prévoyant notamment sa résiliation) sans pénalité pour le COMMANDITAIRE en cas de perte de la qualification SecNumCloud.

Les Services ne comprennent pas d’obligation de réversibilité (à savoir, l’aide au Client pour qu’il puisse migrer son système vers un autre” Prestataire) à l’exception de la mise à disposition du COMMANDITAIRE par le Prestataire de l’interface COMMANDITAIRE permettant au COMMANDITAIRE de sauvegarder et récupérer ses données y compris notamment les données de configuration de leur système d’information via l’une des modalités techniques suivantes au choix du COMMANDITAIRE : la mise à disposition de fichiers suivant un ou plusieurs formats documentés et exploitables en dehors du service fourni par le Prestataire ou bien via la mise en place d’interfaces techniques permettant l’accès aux données suivant un schéma documenté et exploitable (API).

Le COMMANDITAIRE, seul maître de son système, doit tout mettre en œuvre pour faciliter cette opération en tant que de besoin (ce qui implique, notamment, qu’il mette en place une documentation rigoureuse à cet effet) et l’élaboration de plans de réversibilité. Dans le cas où le COMMANDITAIRE aurait besoin d’une prestation complémentaire, le Prestataire peut proposer une mission de conseil à cet égard dans le cadre d’un contrat spécifique à négocier.

# 11. Disponibilité, continuité et restauration du service

## 11.1. Gestion des Incidents et des interruptions

### 11.1.1. Incidents

#### 11.1.1.1. Types d’Incidents traités dans le cadre de cette Convention de service

* Sinistres
* Pannes et défaillances
* Incidents de sécurité :
* Impactant la disponibilité du service
* Impactant la confidentialité du service
* Impactant l’intégrité du service

#### 11.1.1.2. Traitement des incidents

* Délais
* Actions a posteriori
* Archiver les documents détaillant les incidents de sécurité.
* Notification de violation de connées à caractère personnel (en ligne) : <https://notifications.cnil.fr/notifications/index>

#### 11.1.1.3. Niveau de notification des Incidents de sécurité

Le COMMANDITAIRE a la responsabilité de choisir les niveaux de gravité des Incidents de sécurité pour lesquels il souhaite être informé, par exemple via leur formalisation dans un PAS applicable au Service.

Par défaut, le COMMANDITAIRE est informé :

* Des incidents de sécurité avec impact (impacts I1 et I2 selon l’échelle d’impact définie dans le processus de priorisation des traitements de la présente Convention de service) ;
* Des violations de données à caractère personnel pour lesquelles le COMMANDITAIRE est responsable du traitement ;
* Des violations de données à caractère personnel pour lesquelles le Prestataire est responsable du traitement et comportant des données personnelles du COMMANDITAIRE.

## 11.2. Maintenance du Service

### 11.2.1. Nature de la maintenance

La maintenance assurée consiste en la mise en œuvre :

* Du plan de maintien en conditions opérationnelles du Service pour assurer de bons indicateurs de disponibilité tels que s’y engage le Prestataire plus haut ;
* Du plan de PCA/PRA si souscrit par le COMMANDITAIRE déclenché selon les éventuels incidents qui surviendraient.

### 11.2.2. Accès distants de Cloud Temple sur le périmètre du COMMANDITAIRE

Le Prestataire s’interdit, dans le cadre de la présente Convention de service, tout accès aux Tenants et à l’espace de l’interface du COMMANDITAIRE.

Il incombera au COMMANDITAIRE donner les accès nécessaires au personnel du Prestataire. Le COMMANDITAIRE reconnaît que les accès seront utilisés dans le cadre de l’hébergement et in fine de l’infogérance (si souscrit par le COMMANDITAIRE).

### 11.2.3. Accès distants de tiers participant à la fourniture du service sur le périmètre du COMMANDITAIRE

Aucun accès distant de tiers participant à la fourniture du Service n’est autorisé.

Si un besoin technique rendait ce cas de figure nécessaire, alors ce type d’accès ne serait réalisé qu’après notification du COMMANDITAIRE justification et obtention de son accord écrit.

# 12. Procédure d’effacement des données en fin de Contrat

A la fin du Contrat, que le Contrat soit arrivé à son terme ou pour toute autre cause, le Prestataire assura l’effacement sécurisé de l’intégralité des données traitées dans le cadre du Service, y compris les Données techniques du COMMANDITAIRE. Le Prestataire donnera un préavis formel en respectant un délai de vingt et un jours (21) calendaires. Les données du COMMANDITAIRE seront supprimées dans un délai maximum de trente (30) jour après la notification. Le Prestataire fournit un certificat de suppression de données au COMMANDITAIRE.

# 13. Droit applicable

## 13.1. De manière générale

Le droit applicable et auquel est soumise la présente Convention de service est le droit français.

## 13.2. Respect du droit et des réglementations applicables

Le Prestataire s’engage sur les points suivants :

* L’identification des contraintes légales et réglementaires applicables dans le cadre du Service ;
* Le respect des contraintes légales et réglementaires applicables aux données confiées au Prestaire ;
* Le respect de la Loi informatique et liberté et du RGPD ;
* La mise en œuvre de moyens de protection des données personnelles ;
* La mise en œuvre d’un processus de veille légale et réglementaire ;
* De disposer et maintenir des relations appropriées ou une veille avec les autorités sectorielles en lien avec la nature des données traitées dans le cadre du Services. Cela inclus notamment l’ANSSI, le CERT-FR et la CNIL.

## 13.3. RGPD

Agissant en qualité de sous-traitant au sens de l’article 28 du Règlement général sur la protection des données (RGPD), le Prestataire s’engage :

* A assurer la transparence et la traçabilité ;
* A désigner un DPO en charge de définir et mettre en œuvre les mesures de protection des données à caractère personnel ;
* Apporter une assistance et du conseil au COMMANDITAIRE en l’alerte si une instruction de ce dernier constitue une violation des règles de protection des données personnelles si le Prestataire a le moyen d’en identifier ;
* Une garantie de sécurité sur les données traitées (du fait de la qualification SecNumCloud).

## 13.4. Protection vis à vis du droit extra-européen

En cas de recours par le Prestataire, dans le cadre du Service, au service d’une société tierce - y compris un sous-traitant - possédant son siège statutaire, administration centrale ou principal établissement au sein d’un État non membre de l’Union Européenne ou appartenant ou étant contrôlée par une société tierce domiciliée en dehors l’Union Européenne, le Prestataire s’engage que cette susdite société tierce ne disposera d’aucun accès aux données opérées par le service ‘Secure Temple’.

Pour rappel, les données visées sont celles qui sont confiées au Prestataire par le COMMANDITAIRE ainsi que toutes Données techniques comprenant des informations sur les COMMANDITAIRES.

Pour les besoins du présent article, la notion de contrôle est entendue comme étant celle mentionnée au II de l’article L233-3 du code de commerce.

# 14. SIGNATURES

Fait à \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, le \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Pour Cloud Temple, le PRESTATAIRE

Pour \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, le COMMANDITAIRE