Table of Contents

\*\* Table of contents \*\*

* [1.Framework] (#X09AF6387E1D2792B8EDC09FC15ABD136A837DB5)
* [2.Acronyms] (#XC79D173393C04B42BA8CDF223CCA3C0202F4DEE)
* [3.Glossary] (#x0C9D1D82FDC5FCC3D01A320DD2DD3715A6900B4)
* [4.Object of the paas service agreement of Provider] (#X23C3C3767539F9E69CC7CBF5AF8AA8C1B6AD7)
* [5.Evolution of the service agreement PAAS] (#XA7161677DCF9A35D02C20807040326B39D55881)
* [6.Audit] (#x910E2801262de94Af71544B8FB509CC70CC79A)
* [7.DESCRIPTION OF THE SERVICE] (#X3D12A6C93683F0122F5F9A8E21E7C12FC92490B)
* [8.Implementation of Service] (#XC98FB6DA582D483E300ADD6A80DF6E3EB76498A)
* [8.1.Description of components Techniques] (#XA61C340E3FDF14082CEF411D3A913FC4BDEEB4C)
* [8.1.1.Redhat service platform OPENSHIFT] (#XF81D22ED0ABCA8EAB163C160107FA228901D82C)
* [8.1.2.Platform piloting software infrastructure REDHAT OPENSHIFT] (#XF11C2E6A431AE11852FE3129245B4D0FD0747B)
  + [8.1.3. Infrastructure de sauvegarde associée](#X77b1112fa2c2a53eb0cf09b416962164b77b437)
  + [8.1.4. Mise en œuvre de solutions de reprise d'activité ou de continuité d'activité](#Xae1394210f1c9bee4293a93160d2d11cc70ebdd)
* [9. Engagements et niveaux de services](#Xad2b4ae071a52a99b502c4e84cbba3f15ac78f8)
  + [9.1. Engagements de disponibilité de la plateforme RedHat OpenShift](#X273341276df81e9f6fad2000ac84216560e59fa)
* [10. Modèle de responsabilités partagées Applicable] (#XA90D4E180CA2AE1D92E4E4CF00F20ACA5061EAC)
* [10.1.Responsibility and obligations of Provider] (#XE5CF73850EA2189AB60F41560BF52E97D3019F9)
* [10.2.Limitation of responsibility for Provider] (#x8856c8f606130116944398b244484722823c023c)
* [10.3.Limitation access] (#x902763258f1242326933ce46892d3f549e73e30)
* [11.Erasure of data at the end of contract] (#xbe642A80027ce4AD8888C932E98B8661C2A0D3A6)
* [12.Applicable law] (#XA219184D62EB90DFEEC612801FD05C5D816C331)

## 1. Framework

|  |
| --- |
| Reference CT.AM.JUR.Anx.paas 2.1 |
| Date January 21, 2025 |

## 2. Acronyms

| Acronym Description |
| --- |
| CAB Change Advisory Board - Advisory Committee on Changes |
| CMDB Configuration Management Database - Management database configurations |
| Copil Steering Committee |
| Costrat Strategic Committee |
| DB Database (database) |
| DRP Disaster Recovery Plan (Activity recovery plan) GTI Garantie de Temps d’Intervention |
| GTR Garantie de Temps de Résolution |
| GTE Garantie de Temps d’Escalade |
| HYPERVISEUR Système d'exploitation permettant l'execution de VM sur une lame de calcul |
| ITIL Information Technology Infrastructure Library - Bonnes pratiques pour la gestion des systèmes d'information |
| IAAS Infrastructure as a Service |
| MCO Maintien en condition opérationnelle |
| MOA Maitrise d’Ouvrage |
| MOE Maitrise d’Œuvre |
| OS Operating system |
| PAQ Plan d’Assurance Qualité |
| PAAS Platform as a Service |
| SDM Service Delivery Manager |
| 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 - Deadline for the reinstatement of the service disaster case |
| SLA Service Level Agreement - Service level agreement |
| UO Unit of work |
| VABF Validation of aptitude for proper functioning |
| VAB validation of aptitude for good exploitability |
| VM Virtual Machine (Virtual Machine) |
| VSR Validation of regular service |
| SNC SecnumCloud |

## 3. Glossary

The following expressions used in this document will be interpreted in accordance with the definitions assigned to them below :

| Expression Definition |
| --- |
| “Secure Temple " designates the Iaas qualified SecnumCloud service, proposed by Cloud Temple, as defined in the certificate available on the ANSSI website and provided in the appendix to This service agreement. |
| Region a  “region " in the context of cloud computing designates a geographically delimited set of zones of Cloud availability, providing network services, calculation and storage to optimize latency, local performance and regulatory compliance. |
| Zone A specific section and isolated from the infrastructure of Availability (AZ) (Availability Cloud Computing, designed to ensure high availability zone) and the resilience of services by distribution geographic resources. |
| Holding an isolated instance reserved for a user or group users, sharing a common infrastructure everything by maintaining independence and data security and applications. |

| Expression Definition |
| --- |
| Incident an  “incident " designates any unforeseen event which disrupts the normal functioning of a system or compromises data security. |
| Problem a  “problem " is a fundamental cause of one or several incidents, identified or suspected, requiring An analysis and resolution to prevent its recurrence |
| Change a  “change " means any addition, a modification or deletion impacting the service, having been authorized, planned or supported. |
| Change a  “standard change " is a change making standard the subject of a procedure, including the terms of implementation production and impacts (including financial) are known and accepted in advance by the parties.He is then integrated into the catalog of standard changes, and Depending on the case have a GTI and a GTR. Action (s) of the realization of change production when it is approved (the change, in the sense of ITIL, only concerning change management and not its realization/concretization). |
| Request for a request for development subject to a procedure, of which service realization: i) does not modify the CMDB, ii) the mode operative, costs and risks are known and accepted in advance and do not require specific rear return III) The realization is subject to a service level agreement and included in the contract fee when being carried out in working hours and working days. |
| Element of an  “configuration element " is a component identifiable configuration of the information system, such as a logiciel, un matériel ou un document, sujet à gestion dans le cadre de la gestion des services IT |
| Service Un "service" désigne le service qualifié SecNumCloud, délivré au COMMANDITAIRE par le Prestataire, tel que décrit dans la section « Description du Service » de la présente Convention de service. |
| Evenement Un "événement" est toute occurrence détectable ou identifiable that may have an important to management service. |
| Sinister a “disaster” designates a serious event of origin natural or human, accidental or intentional, causing significant losses and damage to the Disaster. |
| Agreement of this document, established within the framework of a contract specific service or general conditions of sale and of use (CGVU), in accordance with Requirements of the SECNUMCLOUD SEP. |
| Availability capacity to ensure the availability and maintenance of optimal performance of a service, in accordance with criteria and commitments defined in the Service level (SLA) |
| Supervision surveillance of an information system or a 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. |

## 4. Objet de la convention de service PaaS du Prestataire

This service agreement establishes the terms and conditions according to which the service provider undertakes to issue to the sponsor a infrastructure in accordance with the specifications of the offer “Platform as a Service - Paas ”, duly qualified SecnumCloud.

Purpose of the service agreement:

1. Specify the performance requirements expected by the sponsor in terms of functionality and reliability of the infrastructure.
2. Énoncer les obligations du Prestataire afin de satisfaire aux niveaux de service convenus.
3. Identifier les normes réglementaires applicables spécifiquement à l'infrastructure proposée.
4. Assurer une uniformité et une intégrité dans l'évaluation de la qualité des services rendus.
5. 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 withdraw its secnumcloud qualification, this contract may be automatically terminated, without incurring penalties, by the Sponsor.In such a possibility, the service provider engages in inform the sponsor of this dequalification by sending a official notification, by means of a registered letter with request of receipt.

It should be noted that a modification or adjustment of the qualification secnumcloud will not be interpreted as a revocation of initial qualification.

## 5. Evolution of the PaaS service agreement

Changes or additions to this service agreement result exclusively from requests formulated by the organs of governance designated for this purpose.These change proposals will be examined within the strategic committee, the only body empowered to Determine the aspects requiring written formalization.

It is agreed that any evolution of the agreement, after validation, which alters the initially established financial conditions, will require the establishment and the signature of an amendment to the current contract.

The factors that may induce a revision of this agreement include, without limiting:

* Adaptation of the PaaS platform orchestrated by the provider.
* The adjustments made to the services deployed by the service provider.
* Variations in commitments made and applicable sanctions.
* organizational reconfigurations within the sponsor or Provider.
* expansion or reduction in the field of application of services to whom the sponsor has subscribed.

The management of versions and revisions of the agreement is recorded In the preamble to the document to facilitate monitoring.

## 6. Audit

The service provider undertakes to allow the sponsor, or to everything third -party listener that the latter would have appointed, to consult the ensemble documents necessary for the certificate of full compliance with Obligations related to compliance with the provisions of Article 28 the General Data Protection Regulations (GDPR), facilitating Thus the realization of audits.

\*\* The provider undertakes in particular to make available to the Sponsor the list of all third parties who can access the data and inform him of any change of subcontractors. \*\*

By the acceptance of this service agreement, the Sponsor gives his explicit authorization to:

1. \*\* The National Agency for Information Systems Systems (ANSSI) \*\* as well as the competent qualification entity for undertake the verification of the conformity of the service and its Information system to standards defined by the repository SecnumCloud.
2. \*\* An audit provider in information systems safety \*\*, duly qualified and expressly designated by the service provider, for carry out security audits relating to the service issued by the provider.

## 7. Service description

The service offer offered by the service provider is characterized by the provision of the following services, which are aligned with The principle of detailed shared responsibility in established standards by the SecnumCloud repository:

* The provision of a Redhat container management platform OpenShift piloted by the service provider. It is understood that the service provider will mobilize his expertise to achieve benefits according to best professional practices, in accordance with their specifications and respecting the standards of its ISO/IEC 27001 certification as well as standard guidelines SecnumCloud.

## 8. Implementation of the service

It is specified that all operations and components physical involved in the provision of qualified service, including This agreement is the subject of, are located in the European Union. This includes support, operational supervision and Safety supervision (SOC).

### 8.1.Description of technical components

PAAS (Platform as a service) service encompasses the entirety of components and services required for optimal operation in the Respect for the secnumcloud qualification.

In this regard, their performance and reliability are intrinsically linked Technical components and services of \*\* Iaas \*\* infrastructure of the service provider, as specified in the document [Service agreement Iaas] (../ working%20in%20Progress%20-%20NOT%20use/IAAS/SLA\_IAAS.MD) Provider.

### 8.1.1.Redhat Openshift Redhat Service Platform

The service includes the provision within a region, out of 3 availability zones,

### 8.1.2.Redenshift Redhat Platform Infrastructure

Le Prestataire fournit au COMMANDITAIRE la console d'administration et l'API nécessaire à l'exploitation de ses environnements PaaS RedHat OpenShift. Il s'engage également à les maintenir en condition opérationnelle optimale et à assurer sa sécurité de manière continue.

Dans le cadre spécifique du service fourni, le Prestataire met à la disposition du COMMANDITAIRE toutes les interfaces et API de la plateforme RedHat OpenShift au sein du tenant sélectionné. Il revient au COMMANDITAIRE d'instaurer les dispositifs de sécurité appropriés, tels que les pare-feux (firewall), les pare-feux applicatifs Web (WAF), et autres mesures de protection, ainsi que de définir les règles de filtrage associées pour sécuriser l'accès à sa plateforme conformément à sa politique de sécurité.

Le Prestataire alerte le COMMANDITAIRE sur le fait qu'une utilisation anormale de sa console d'administration, notamment en cas de surcharge of his command apis (Hammering), can trigger measures of automatic safety resulting in blocking access to the APIs of order or certain services of the service provider.It is advisable to underline that this situation does not constitute unavailability of the service but a protection action for the provider’s infrastructure;by consequently, the sponsor cannot consider it as a unavailability in its calculations. In addition, the service provider specifies to the sponsor that requests perfectly identical (duplicates) sent to its APIS are limited to One per second (Throttling).If the sponsor submits requests identical to a higher frequency, their rejection should not be interpreted as unavailability of the service.

### 8.1.3.Associated backup infrastructure

The service provider provides the sponsor with a integrated, dedicated and managed backup, intended for the protection of data from its Redhat OpenShift environments.The service provider provides maintenance in operational condition and safety condition of This integrated backup platform.Regardless of the number of availability zones subscribed by the sponsor, the service provider ensures that the sponsor’s backup platform will be located in Outside the availability area of ​​safeguarded workloads. The backup service is limited to saving machines virtuals and topology configurations of the IAAS environment SECNUMCLOUD supporters of the sponsor.Development and the application of an adequate backup policy by the Sponsor depend on the subscription to work units specific.It is therefore the responsibility of the sponsor to ensure the availability of the necessary technical resources with the Provider to implement their safeguard policy or to adjust the latter according to the means available.

The service provider undertakes to notify the sponsor in the event of capacity constraints and to provide advice assistance for the optimization of resources.The provider’s obligations are will limit to the implementation of the needs expressed by the sponsor in terms of safeguard policy, within the framework of resources subscribed. ### 8.1.4.Implementation of resumption of activity or activity continuity

The service provider provides the sponsor with the set of solutions techniques necessary to guarantee an optimal distribution of its resources through various availability areas.It is the responsibility of Sponsor the responsibility to effectively manage this distribution of resources, for which he has the possibility to exploit the tools of the provider available for this use. In particular, applications deployed on the Redhat platform OpenShift must take care of the redundancy mechanisms proposed by the service provider in order to be able to benefit from the solutions of Resumption of activity or associated activity continuity.

## 9. Commitments and service levels

The service provider undertakes to guarantee continuous monitoring of the performance and the security integrity of its platforms and services, ensuring their optimal operation. The unavailability of a service, being subject to an indicator of performance, is recognized as soon as it is identified by the system of supervision of the service provider, or following a notification by a sponsor user.The beginning of unavailability is fixed at the earliest moment between these two events, in order to guarantee a precise count and just unavailability time.

The end of unavailability is officially marked by the full restoration of the service, confirmed either by the tools of supervision of the service provider, either by user return, ensuring thus an effective recovery of operations and a faithful measure of the duration of interruption.

### 9.1.Availability commitments of the Redhat Openshift platform

The service provider undertakes to maintain a level of availability and performance in accordance with the standards defined for each period specified.Service level commitments (Level Service Agreements, SLAS) apply provided that the sponsor implements its systems through at least two of the areas of availability present in the region concerned.

In the absence of compliance with these conditions by the sponsor, He will be inability to claim the application of SLAS concerned, which are specifically identified by a Asterisk (\*).Accessibility to SLAS is done via the interface Sponsor.\*\* The measures hear calculated monthly \*\*:

-\*\*SLA 1 (\*): IC-PAAS\_SNC-01 \*\*-Availability of the platform Redhat Openshift: guaranteed availability rate of 99.9%, calculated on A 24 -hour base, 7 days a week.

***Remarks*** :

* *In response an attack by denial of distributed service (DDOS), the Provider reserves the right to adjust its routing configuration Internet to limit the impact of this attack and save its infrastructure.In particular, if an IP address belonging to Sponsor is targeted, the service provider can use the technique of Blackholing via the BGP community to block all traffic to the IP address referred to upstream to its suppliers, in order to protect the resources of the sponsor as well as those of others Sponsors and infrastructure of the service provider.The provider strongly encourages the sponsor to adopt similar measures, such as using web applications firewall software available on the market, and to carefully configure its groups security via the control api.*
* *The service provider insists on the need for the sponsor of minimize flow openings, notably avoiding making Accessible the administration ports*  ***SSH***  *(Port TCP 22) and*  ***RDP***  *(TCP port 3389) from the Internet set (Sub-network 0.0.0.0/0), as well as internal protocols such as*  ***SMB***  *(port TCP/UDP 445) or*  ***NFS***  *(TCP/UDP 2049 port).*

## 10. Applicable shared responsibility model

### 10.1.Provider’s responsibility and obligations

The service provider undertakes to provide the sponsor of user interfaces in French and English language, thus facilitating l'accès et la gestion des services fournis. Le COMMANDITAIRE, de son côté, s'engage à respecter les contraintes légales et réglementaires en vigueur relatives aux données qu'il confie au Prestataire pour traitement.

En cas de transmission de données sujettes à des exigences légales spécifiques, le Prestataire collaborera avec le COMMANDITAIRE pour identifier et mettre en œuvre les mesures de sécurité nécessaires, conformément aux obligations du Prestataire et dans le cadre de la provision of services.

The provider also takes the commitment to examine and take in consideration the specific needs linked to the activity sectors of the sponsor, respecting the limitations of his responsibility, To guarantee a level of security adapted to the information processed.

If a project is likely to impact the security of the service offered or the availability of said service or to generate a loss of functionality, the service provider undertakes to inform through the console or by email in contact with the sponsor and within a reasonable time the sponsor of potential impacts, corrective measures envisaged and residual risks which concerns him, ensuring a total transparency.

The service provider undertakes not to use the data from the sponsor from production to carry out tests, with the exception of obtain the explicit authorization of the sponsor beforehand, to whom cases the provider undertakes to anonymize this data and ensure its confidentiality during their anonymization.

In the event of a change of subcontractor for accommodation, Provider will inform the sponsor upstream, assuring that this transition does not negatively affect the service provided.

At the request of the sponsor, the service provider will provide access to his internal regulations, to his ethics charter, to applicable sanctions in the event of non-compliance with its security policy, to events the concerning, procedures relating to the service and requirements specific security.

The service provider undertakes to inform the sponsor of any change to come on software elements under the responsibility of Cloud Temple as long as complete compatibility cannot be ensured.

### 10.2.Provider’s liability limitation

The shared liability structure effectively reduces the extent from the intervention of the service provider to the aspects linked to the supply a functional redhat openshift platform, comprising:

* management of the IAAS infrastructure which supports the platform Redhat Openshift and its provisioning,
* the management of the systems necessary for the proper functioning of the platform,
* Maintaining safety conditions,
* Updating the Redhat OpenShift platform,
* the backup of the essential configuration data of this platform, with the exception of data and applications of Sponsor who fall under his responsibility.

She excludes in particular, but without limiting herself:

* Updating of operating systems and installed software by the sponsor on its OpenShift environments in its spaces rental,
* the security of programs, software and applications installed in within the OpenShift environment by the sponsor,
* data backup at the application level,
* The configuration of safeguard policies.

### 10.3.Access limitation

As part of this service agreement, the service provider is formally prohibited to access the proponents belonging to the Sponsor without prior authorization.It is responsibility of the sponsor to provide the necessary access to the staff of Provider, according to the specific needs of accommodation and the case related, professional support services, if this option has been chosen by the sponsor.

The sponsor acknowledges that these access is granted exclusively for needs related to the provision of agreed services, ensuring Thus a secure management and in accordance with the terms of the agreement.

Distant access by third parties involved in the provision of service of the provider is strictly prohibited.In the event that a specific technical requirement would require such access, this could be established that after clearly notified the Sponsor, provided a detailed justification and obtained his agreement writing.

This measure guarantees the control and security of data from Sponsor, ensuring that any exception to the rule is duly authorized and documented.

## 11. Erase data at the end of the contract

At the end of the contract, that it matters or that it is terminated for any reason, the service provider undertakes to proceed to The secure erasure of the entire data of the sponsor, Y including technical data.The provider will ensure communicate to the sponsor a formal notice, respecting a period of Twenty -one (21) calendar days.The data of the sponsor will be then deleted within a maximum period of thirty (30) days following This notification.

To attest to this deletion, the provider will give to the Sponsor A certificate confirming the erasure of the data.

## 12. Applicable law

The law applicable for the present service agreement is the law French.

In the event of appeal by the service provider, as part of the services provided to the sponsor, to a third-party company, including a subcontractor, of which the head office, central administration or the main establishment is located in a non -member of the European Union, or who is property or under the control of a third -party company domiciled outside the European Union, the service provider is committed to ensure that said company third will have no access to data processed by the service provider.

It should be noted that the data referred to that includes those entrusted to Provider by the sponsor, as well as all the data techniques such as identities of beneficiaries and Administrators of the technical infrastructure, the data manipulated by networks, newspapers of technical infrastructure, directory, certificates, access configuration, etc., containing information on the sponsor.

For precision, the concept of control is defined in accordance with the II of Article L233-3 of the Commercial Code.